Scan Report

May 26, 2017

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "DVL". The scan started at Fri May 26 13:20:06 2017 UTC and ended at Fri May 26 14:06:43 2017 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview **2**

1.1 Host Authentications 2

2 Results per Host **2**

2.1 192.168.27.45 2

2.1.1 High general/tcp 3

2.1.2 High 22/tcp 374

2.1.3 High 80/tcp 381

2.1.4 Medium general/tcp 467

2.1.5 Medium 22/tcp 601

2.1.6 Medium 631/tcp 607

2.1.7 Medium 80/tcp 609

2.1.8 Medium 5432/tcp 681

2.1.9 Low general/tcp 682

2.1.10 Low 22/tcp 692

2.1.11 Low 80/tcp 695

2.1.12 Log general/tcp 701

2.1.13 Log 6001/tcp 725

2.1.14 Log 69/udp 726

2.1.15 Log 22/tcp 726

2.1.16 Log 5801/tcp 730

2.1.17 Log 3306/tcp 731

2.1.18 Log 5901/tcp 732
2.1.19 Log general/icmp 733
2.1.20 Log 631/tcp 734
2.1.21 Log 5001/tcp 737
2.1.22 Log 80/tcp 738
2.1.23 Log 6000/tcp 753
2.1.24 Log general/CPE-T 753

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.27.45	490	273	24	84	0
Total: 1	490	273	24	84	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.

This report contains all 871 results selected by the filtering described above. Before filtering there were 871 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.27.45	SSH	Success	Protocol SSH, Port 22, User root

2 Results per Host

2.1 192.168.27.45

Host scan start Fri May 26 13:20:22 2017 UTC
Host scan end Fri May 26 14:06:43 2017 UTC

Service (Port)	Threat Level
general/tcp	High
22/tcp	High
80/tcp	High
general/tcp	Medium
22/tcp	Medium
631/tcp	Medium
80/tcp	Medium
5432/tcp	Medium
general/tcp	Low
22/tcp	Low
80/tcp	Low
general/tcp	Log
6001/tcp	Log
69/udp	Log
22/tcp	Log

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
5801/tcp	Log
3306/tcp	Log
5901/tcp	Log
general/icmp	Log
631/tcp	Log
5001/tcp	Log
80/tcp	Log
6000/tcp	Log
general/CPE-T	Log

2.1.1 High general/tcp

High (CVSS: 9.3)
NVT: Adobe Acrobat and Reader PDF Handling Code Execution Vulnerability (Linux)

Product detection result
`cpe:/a:adobe:acrobat_reader:7.0.5`
`Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0`
`↪.800108)`

Summary
This host is installed with Adobe Reader and is prone to remote code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code by tricking a user into opening a PDF file embedding a malicious Flash animation and bypass intended sandbox restrictions allowing cross-domain requests.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader version 9.3.1 or 8.2.1 or later. For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Reader version 8.x before 8.2.1 and 9.x before 9.3.1 on Linux.

Vulnerability Insight
Flaw is caused by a memory corruption error in the 'authplay.dll' module when processing malformed Flash data within a PDF document and some unspecified error.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Acrobat and Reader PDF Handling Code Execution Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.902129
Version used: $Revision: 5394 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2010-0188, CVE-2010-0186
BID:38195, 38198
Other:
URL:http://xforce.iss.net/xforce/xfdb/56297
URL:http://www.vupen.com/english/advisories/2010/0399
URL:http://securitytracker.com/alerts/2010/Feb/1023601.html
URL:http://www.adobe.com/support/security/bulletins/apsb10-07.html

High (CVSS: 9.3)
NVT: Adobe Acrobat and Reader PDF Handling Code Execution Vulnerability (Mac OS X)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host is installed with Adobe Reader/Acrobat and is prone to remote code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code by tricking a user into opening a PDF file embedding a malicious Flash animation and bypass intended sandbox restrictions allowing cross-domain requests.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to Adobe Reader/Acrobat version 9.3.1 or 8.2.1 or later. For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Reader version 8.x before 8.2.1 and 9.x before 9.3.1 on Mac OS X. Adobe Acrobat version 8.x before 8.2.1 and 9.x before 9.3.1 on Mac OS X

Vulnerability Insight
Flaw is caused by a memory corruption error in the 'authplay.dll' module when processing malformed Flash data within a PDF document and some unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Acrobat and Reader PDF Handling Code Execution Vulnerability (Mac OS X)`
OID:1.3.6.1.4.1.25623.1.0.804267
Version used: `$Revision: 2482 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
`CVE: CVE-2010-0188, CVE-2010-0186`
`BID:38195, 38198`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/56297`
`URL:http://www.vupen.com/english/advisories/2010/0399`
`URL:http://securitytracker.com/alerts/2010/Feb/1023601.html`
`URL:http://www.adobe.com/support/security/bulletins/apsb10-07.html`

High (CVSS: 9.3)
NVT: Adobe Acrobat and Reader PDF Handling Code Execution Vulnerability (Windows)

Product detection result
`cpe:/a:adobe:acrobat_reader:7.0.5`
`Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0`
`↪.800108)`

Summary
This host is installed with Adobe Reader/Acrobat and is prone to remote code execution vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code by tricking a user into opening a PDF file embedding a malicious Flash animation and bypass intended sandbox restrictions allowing cross-domain requests.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader/Acrobat version 9.3.1 or 8.2.1 or later. For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Reader version 8.x before 8.2.1 and 9.x before 9.3.1 Adobe Acrobat version 8.x before 8.2.1 and 9.x before 9.3.1

Vulnerability Insight
Flaw is caused by a memory corruption error in the 'authplay.dll' module when processing malformed Flash data within a PDF document and some unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Acrobat and Reader PDF Handling Code Execution Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.902128
Version used: `$Revision: 5394 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
`CVE: CVE-2010-0188, CVE-2010-0186`
`BID:38195, 38198`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/56297`
`URL:http://www.vupen.com/english/advisories/2010/0399`
`URL:http://securitytracker.com/alerts/2010/Feb/1023601.html`
`URL:http://www.adobe.com/support/security/bulletins/apsb10-07.html`

High (CVSS: 9.3)
NVT: Adobe Acrobat and Reader SING 'uniqueName' Buffer Overflow Vulnerability (Linux)

Product detection result
`cpe:/a:adobe:acrobat_reader:7.0.5`

... continues on next page ...

... continued from previous page ...

Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0 ↪.800108)

Summary
This host is installed with Adobe Reader and is prone to buffer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to crash an affected application or execute arbitrary code by tricking a user into opening a specially crafted PDF document.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader version 9.4, For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Reader version 9.3.4 and prior.

Vulnerability Insight
The flaw is due to a boundary error within 'CoolType.dll' when processing the 'uniqueName' entry of SING tables in fonts.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Acrobat and Reader SING 'uniqueName' Buffer Overflow Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.801516
Version used: $Revision: 5263 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2010-2883
BID:43057
Other:
URL:http://secunia.com/advisories/41340
URL:http://www.adobe.com/support/security/advisories/apsa10-02.html
URL:http://blog.metasploit.com/2010/09/return-of-unpublished-adobe.html

High (CVSS: 9.3)
NVT: Adobe Acrobat and Reader SING 'uniqueName' Buffer Overflow Vulnerability (Windows)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host is installed with Adobe Reader/Acrobat and is prone to buffer overflow vulnerability

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to crash an affected application or execute arbitrary code by tricking a user into opening a specially crafted PDF document.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader/Adobe Acrobat version 9.4 or later. For updates refer http://www.adobe.com/downloads/

Affected Software/OS
Adobe Reader version 9.3.4 and prior. Adobe Acrobat version 9.3.4 and prior on windows.

Vulnerability Insight
The flaw is due to a boundary error within 'CoolType.dll' when processing the 'uniqueName' entry of SING tables in fonts.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Acrobat and Reader SING 'uniqueName' Buffer Overflow Vulnerability (Windo.
↪..
OID:1.3.6.1.4.1.25623.1.0.801515
Version used: $Revision: 5263 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2010-2883
BID:43057

. . . continues on next page . . .

. . . continued from previous page . . .

```
Other:
  URL:http://secunia.com/advisories/41340
   URL:http://www.adobe.com/support/security/advisories/apsa10-02.html
   URL:http://blog.metasploit.com/2010/09/return-of-unpublished-adobe.html
```

High (CVSS: 9.3)
NVT: Adobe Flash Player 9.0.115.0 and earlier vulnerability (Linux)

Summary
The remote host is probably affected by the vulnerabilities described in CVE-2007-5275, CVE-2007-6019, CVE-2007-6243, CVE-2007-6637, CVE-2008-1654, CVE-2008-1655

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
CVE 2007-5275 The Adobe Macromedia Flash 9 plug-in allows remote attackers to cause a victim machine to establish TCP sessions with arbitrary hosts via a Flash (SWF) movie, related to lack of pinning of a hostname to a single IP address after receiving an allow-access-from element in a cross-domain-policy XML document, and the availability of a Flash Socket class that does not use the browser's DNS pins, aka DNS rebinding attacks, a different issue than CVE-2002-1467 and CVE-2007-4324. CVE 2007-6019 Adobe Flash Player 9.0.115.0 and earlier, and 8.0.39.0 and earlier, allows remote attackers to execute arbitrary code via an SWF file with a modified DeclareFunction2 Actionscript tag, which prevents an object from being instantiated properly. CVE 2007-6243 Adobe Flash Player 9.x up to 9.0.48.0, 8.x up to 8.0.35.0, and 7.x up to 7.0.70.0 does not sufficiently restrict the interpretation and usage of cross-domain policy files, which makes it easier for remote attackers to conduct cross-domain and cross-site scripting (XSS) attacks. CVE 2007-6637 Multiple cross-site scripting (XSS) vulnerabilities in Adobe Flash Player allow remote attackers to inject arbitrary web script or HTML via a crafted SWF file, related to 'pre-generated SWF files' and Adobe Dreamweaver CS3 or Adobe Acrobat Connect. NOTE: the asfunction: vector is already covered by CVE-2007-6244.1. CVE 2008-1654 Interaction error between Adobe Flash and multiple Universal Plug and Play (UPnP) services allow remote attackers to perform Cross-Site Request Forgery (CSRF) style attacks by using the Flash navigateToURL function to send a SOAP message to a UPnP control point, as demonstrated by changing the primary DNS server. CVE 2008-1655 Unspecified vulnerability in Adobe Flash Player 9.0.115.0 and earlier, and 8.0.39.0 and earlier, makes it easier for remote attackers to conduct DNS rebinding attacks via unknown vectors.

Solution
All Adobe Flash Player users should upgrade to the latest version:

Vulnerability Detection Method
Details:`Adobe Flash Player 9.0.115.0 and earlier vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.90018
Version used: `$Revision: 5661 $`

References

. . . continues on next page . . .

... continued from previous page ...

CVE: CVE-2007-5275, CVE-2007-6019, CVE-2007-6243, CVE-2007-6637, CVE-2008-1654, CVE-2008-1655
BID:28697, 28696, 27034, 26966, 28694, 26930

High (CVSS: 9.3)
NVT: Adobe Flash Player Arbitrary Code Execution Vulnerability (Linux)

Summary
This host has Adobe flash Player installed, and is prone to code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to corrupt memory and execute arbitrary code on the system with elevated privileges.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade adobe flash player to version 10.2.159.1 or later, Update Adobe Reader/Acrobat to version 9.4.4 or 10.0.3 or later, For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Flash Player version 10.2.153.1 and prior on Linux

Vulnerability Insight
The flaw is due to an error in handling 'SWF' file in adobe flash player, which allows attackers to execute arbitrary code or cause a denial of service via crafted flash content.

Vulnerability Detection Method
Details:Adobe Flash Player Arbitrary Code Execution Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.801922
Version used: $Revision: 5424 $

References
CVE: CVE-2011-0611
BID:47314
Other:
URL:https://www.kb.cert.org/vuls/id/230057
URL:http://www.adobe.com/support/security/advisories/apsa11-02.html
URL:http://blogs.adobe.com/psirt/2011/04/security-advisory-for-adobe-flash-player-adobe-reader-and-acrobat-apsa11-02.html

High (CVSS: 9.3)
NVT: Adobe Flash Player Arbitrary Code Execution Vulnerability (Linux)

Summary
This host has Adobe flash Player installed, and is prone to code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to corrupt memory and execute arbitrary code on the system with elevated privileges.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade adobe flash player to version 10.2.159.1 or later, Update Adobe Reader/Acrobat to version 9.4.4 or 10.0.3 or later, For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Flash Player version 10.2.153.1 and prior on Linux

Vulnerability Insight
The flaw is due to an error in handling 'SWF' file in adobe flash player, which allows attackers to execute arbitrary code or cause a denial of service via crafted flash content.

Vulnerability Detection Method
Details:`Adobe Flash Player Arbitrary Code Execution Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.801922
Version used: `$Revision: 5424 $`

References
```
CVE: CVE-2011-0611
BID:47314
Other:
  URL:https://www.kb.cert.org/vuls/id/230057
   URL:http://www.adobe.com/support/security/advisories/apsa11-02.html
   URL:http://blogs.adobe.com/psirt/2011/04/security-advisory-for-adobe-flash-pl
↪ayer-adobe-reader-and-acrobat-apsa11-02.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Arbitrary Code Execution Vulnerability - 01 Feb14 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

. . . continues on next page . . .

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to arbitrary code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to, execute arbitrary code and cause buffer overflow.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.336 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player versions before 11.2.202.336 on Linux

Vulnerability Insight
Flaw is due to an integer underflow condition that is triggered as unspecified user-supplied input is not properly validated.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Arbitrary Code Execution Vulnerability - 01 Feb14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804087
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2014-0497`
`BID:65327`
`Other:`
`URL:http://secunia.com/advisories/56737`
`URL:http://helpx.adobe.com/security/products/flash-player/apsb14-04.html`
`URL:http://krebsonsecurity.com/2014/02/adobe-pushes-fix-for-flash-zero-day-at`
`↪tack`

High (CVSS: 10.0)
NVT: Adobe Flash Player Arbitrary Code Execution Vulnerability - 01 Feb14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to arbitrary code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to, execute arbitrary code and cause buffer overflow.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.336 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player versions before 11.2.202.336 on Linux

Vulnerability Insight
Flaw is due to an integer underflow condition that is triggered as unspecified user-supplied input is not properly validated.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Arbitrary Code Execution Vulnerability - 01 Feb14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804087
Version used: $Revision: 3521 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0497
BID:65327
Other:

. . . continues on next page . . .

... continued from previous page ...

URL:http://secunia.com/advisories/56737
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-04.html
URL:http://krebsonsecurity.com/2014/02/adobe-pushes-fix-for-flash-zero-day-at
↪tack

High (CVSS: 10.0)
NVT: Adobe Flash Player Buffer Overflow Vulnerability (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to buffer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause denial of service condition. Impact Level: System/Application

Solution
Solution type: VendorFix

Affected Software/OS
Adobe Flash Player version before 10.3.183.50, 11.x before 11.2.202.261 on Linux
Update to Adobe Flash Player version 10.3.183.50 or 11.2.202.261 or later, For updates refer to http://get.adobe.com/flashplayer

Vulnerability Insight
An integer overflow error within 'flash.display.BitmapData()', which can be exploited to cause a heap-based buffer overflow.

Vulnerability Detection Method
Details:Adobe Flash Player Buffer Overflow Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.803154
Version used: $Revision: 3556 $

References
CVE: CVE-2013-0630
BID:57184
Other:
URL:http://secunia.com/advisories/51771
URL:http://securitytracker.com/id?1027950
URL:http://www.adobe.com/support/security/bulletins/apsb13-01.html

... continues on next page ...

... continued from previous page ...

High (CVSS: 10.0)
NVT: Adobe Flash Player Buffer Overflow Vulnerability (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to buffer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause denial of service condition. Impact Level: System/Application

Solution
Solution type: VendorFix

Affected Software/OS
Adobe Flash Player version before 10.3.183.50, 11.x before 11.2.202.261 on Linux
Update to Adobe Flash Player version 10.3.183.50 or 11.2.202.261 or later, For updates refer to http://get.adobe.com/flashplayer

Vulnerability Insight
An integer overflow error within 'flash.display.BitmapData()', which can be exploited to cause a heap-based buffer overflow.

Vulnerability Detection Method
Details:`Adobe Flash Player Buffer Overflow Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803154
Version used: `$Revision: 3556 $`

References
```
CVE: CVE-2013-0630
BID:57184
Other:
  URL:http://secunia.com/advisories/51771
   URL:http://securitytracker.com/id?1027950
   URL:http://www.adobe.com/support/security/bulletins/apsb13-01.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Buffer Overflow Vulnerability - Apr14 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to buffer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary code and cause a buffer overflow, resulting in a denial of service condition.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.356 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.356 on Linux

Vulnerability Insight
Flaw is due to an improper validation of user-supplied input to the pixel bender component.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Buffer Overflow Vulnerability - Apr14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804561
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2014-0515`
`BID:67092`
`Other:`
`URL:http://secpod.org/blog/?p=2577`
`URL:http://www.securelist.com/en/blog/8212`
`URL:http://helpx.adobe.com/security/products/flash-player/apsb14-13.html`

High (CVSS: 10.0)
NVT: Adobe Flash Player Buffer Overflow Vulnerability - Apr14 (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to buffer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary code and cause a buffer overflow, resulting in a denial of service condition.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.356 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.356 on Linux

Vulnerability Insight
Flaw is due to an improper validation of user-supplied input to the pixel bender component.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Buffer Overflow Vulnerability - Apr14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804561
Version used: $Revision: 3521 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0515
BID:67092
Other:
URL:http://secpod.org/blog/?p=2577
URL:http://www.securelist.com/en/blog/8212
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-13.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Code Execution and DoS Vulnerabilities (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to code execution and denial of service vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.18 or 11.2.202.228 or later, For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version prior to 10.3.183.18 and 11.x to 11.1.102.63 on Linux

Vulnerability Insight
The flaws are due to an unspecified error within the NetStream class.

Vulnerability Detection Method
Details:`Adobe Flash Player Code Execution and DoS Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.903015
Version used: `$Revision: 5950 $`

References
```
CVE: CVE-2012-0772, CVE-2012-0773, CVE-2012-0724, CVE-2012-0725
BID:52748, 52916, 52914
Other:
  URL:http://secunia.com/advisories/48623/
   URL:http://www.securitytracker.com/id/1026859
   URL:http://www.adobe.com/support/security/bulletins/apsb12-07.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Code Execution and DoS Vulnerabilities (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to code execution and denial of service vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

. . . continues on next page . . .

... continued from previous page ...

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.18 or 11.2.202.228 or later, For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version prior to 10.3.183.18 and 11.x to 11.1.102.63 on Linux

Vulnerability Insight
The flaws are due to an unspecified error within the NetStream class.

Vulnerability Detection Method
Details:Adobe Flash Player Code Execution and DoS Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.903015
Version used: $Revision: 5950 $

References
CVE: CVE-2012-0772, CVE-2012-0773, CVE-2012-0724, CVE-2012-0725
BID:52748, 52916, 52914
Other:
URL:http://secunia.com/advisories/48623/
URL:http://www.securitytracker.com/id/1026859
URL:http://www.adobe.com/support/security/bulletins/apsb12-07.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Code Execution and DoS Vulnerabilities Nov13 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to remote code execution and denial of service vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to execute arbitrary code, cause denial of service (memory corruption) and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.327 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.327 on Linux

Vulnerability Insight
Flaws are due to unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Code Execution and DoS Vulnerabilities Nov13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804147
Version used: `$Revision: 3556 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2013-5329, CVE-2013-5330`
`BID:63680, 63680`
`Other:`
`URL:http://secunia.com/advisories/55527`
`URL:http://www.adobe.com/support/security/bulletins/apsb13-26.html`

High (CVSS: 10.0)
NVT: Adobe Flash Player Code Execution and DoS Vulnerabilities Nov13 (Linux)

Product detection result
`cpe:/a:adobe:flash_player:9.0.31.0`
`Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2`
`↪5623.1.0.800032)`

Summary
This host is installed with Adobe Flash Player and is prone to remote code execution and denial of service vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary code, cause denial of service (memory corruption) and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.327 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.327 on Linux

Vulnerability Insight
Flaws are due to unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Code Execution and DoS Vulnerabilities Nov13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804147
Version used: `$Revision: 3556 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2013-5329, CVE-2013-5330`
`BID:63680, 63680`
`Other:`
`URL:http://secunia.com/advisories/55527`
`URL:http://www.adobe.com/support/security/bulletins/apsb13-26.html`

High (CVSS: 9.3)
NVT: Adobe Flash Player Font Parsing Code Execution Vulnerability - (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to unspecified code execution vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause the application to crash and take control of the affected system. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.238 or later, For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version 11.2.202.236 and prior on Linux

Vulnerability Insight
An unspecified error occurs when handling SWF content in a word document. This may allow a context-dependent attacker to execute arbitrary code.

Vulnerability Detection Method
Details:`Adobe Flash Player Font Parsing Code Execution Vulnerability - (Linux)`
OID:1.3.6.1.4.1.25623.1.0.802941
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2012-1535`
`BID:55009`
`Other:`
`URL:http://secunia.com/advisories/50285/`
`URL:http://www.adobe.com/support/security/bulletins/apsb12-18.html`

High (CVSS: 9.3)
NVT: Adobe Flash Player Font Parsing Code Execution Vulnerability - (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to unspecified code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause the application to crash and take control of the affected system. Impact Level: System/Application

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.238 or later, For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version 11.2.202.236 and prior on Linux

Vulnerability Insight
An unspecified error occurs when handling SWF content in a word document. This may allow a context-dependent attacker to execute arbitrary code.

Vulnerability Detection Method
Details:`Adobe Flash Player Font Parsing Code Execution Vulnerability - (Linux)`
OID:1.3.6.1.4.1.25623.1.0.802941
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2012-1535`
`BID:55009`
`Other:`
`URL:http://secunia.com/advisories/50285/`
`URL:http://www.adobe.com/support/security/bulletins/apsb12-18.html`

High (CVSS: 9.3)
NVT: Adobe Flash Player for Linux SWF Processing Vulnerability

Summary
This host has Adobe Flash Player installed and is prone to Shockwave Flash (SWF) Processing vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful attack could result in execution of arbitrary code on the remote affected system. Impact Level: System

Solution
Upgrade to Adobe Flash Player 9.0.152.0 or 10.0.15.3, http://www.adobe.com/downloads

Affected Software/OS
Adobe Flash Player prior to 9.0.152.0/10.0.15.3 on Linux.

Vulnerability Insight
The issue is due to the way Flash Player handles the SWF files.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:Adobe Flash Player for Linux SWF Processing Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800087
Version used: $Revision: 4218 $

References
CVE: CVE-2008-5499
Other:
URL:http://www.adobe.com/support/security/bulletins/apsb08-24.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Improper FLV Parsing Vulnerability June15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to unspecified vulnerability.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 11.2.202.468

Impact
Successful exploitation will allow remote attacker to downloaded a malicious flash file and create a back door results in taking complete control over the victim's system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.468 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player versions before 11.2.202.468 on Linux.

Vulnerability Insight
Flaw is due to improper parsing of Flash Video (FLV) files by Adobe Flash Player.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Improper FLV Parsing Vulnerability June15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805804

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 2582 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-3113
Other:
URL:https://krebsonsecurity.com/tag/cve-2015-3113
URL:https://helpx.adobe.com/security/products/flash-player/apsb15-14.html
URL:http://securityaffairs.co/wordpress/38044/cyber-crime/adobe-fixed-cve-201
↪5-3113.html
URL:https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestin
↪e-wolf-adobe-flash-zero-day.html
URL:http://blog.trendmicro.com/trendlabs-security-intelligence/adobe-issues-e
↪mergency-patch-for-flash-zero-day

High (CVSS: 10.0)
NVT: Adobe Flash Player Improper FLV Parsing Vulnerability June15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to unspecified vulnerability.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.468

Impact
Successful exploitation will allow remote attacker to downloaded a malicious flash file and create a back door results in taking complete control over the victim's system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.468 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Adobe Flash Player versions before 11.2.202.468 on Linux.

Vulnerability Insight
Flaw is due to improper parsing of Flash Video (FLV) files by Adobe Flash Player.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Improper FLV Parsing Vulnerability June15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805804
Version used: `$Revision: 2582 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-3113
Other:
  URL:https://krebsonsecurity.com/tag/cve-2015-3113
   URL:https://helpx.adobe.com/security/products/flash-player/apsb15-14.html
   URL:http://securityaffairs.co/wordpress/38044/cyber-crime/adobe-fixed-cve-201
↪5-3113.html
   URL:https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestin
↪e-wolf-adobe-flash-zero-day.html
   URL:http://blog.trendmicro.com/trendlabs-security-intelligence/adobe-issues-e
↪mergency-patch-for-flash-zero-day
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Security Bypass Vulnerabilities (Linux)

Summary
This host has Adobe Flash Player installed and is prone to multiple security bypass vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful attack could allow malicious people to bypass certain security restrictions or manipulate certain data. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player 10.0.12.36 http://www.adobe.com/downloads/

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Adobe Flash Player 9.x - 9.0.124.0 on Linux

Vulnerability Insight
The flaws are due to, - a design error in the application that allows access to the system's camera and microphone by tricking the user into clicking Flash Player access control dialogs disguised as normal graphical elements. - FileReference.browse() and FileReference.download() methods which can be called without user interaction and can potentially be used to trick a user into downloading or uploading files.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Security Bypass Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800028
Version used: `$Revision: 4218 $`

References
`CVE: CVE-2007-6243, CVE-2008-3873, CVE-2007-4324, CVE-2008-4401, CVE-2008-4503`
`BID:31117`
`Other:`
`URL:http://secunia.com/advisories/32163/`
`URL:http://www.adobe.com/support/security/bulletins/apsb08-18.html`
`URL:http://www.adobe.com/support/security/advisories/apsa08-08.html`
`URL:http://blogs.adobe.com/psirt/2008/10/clickjacking_security_advisory.html`

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause a denial of service via unknown vectors. Impact Level: Application/System

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 10.1.102.64 or later For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version 10.1.85.3 and prior on Linux

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Insight
The flaws are caused by unspecified errors, that can be exploited to execute arbitrary code or cause a denial of service.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.801630
Version used: $Revision: 5263 $

References
CVE: CVE-2010-3636, CVE-2010-3637, CVE-2010-3638, CVE-2010-3639, CVE-2010-3640,
↪CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE
↪-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, CVE-20
↪10-3652
BID:44669
Other:
URL:http://secunia.com/advisories/41917
URL:http://www.adobe.com/support/security/bulletins/apsb10-26.html

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause a denial of service via unknown vectors. Impact Level: Application/System

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 10.1.102.64 or later For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version 10.1.85.3 and prior on Linux

Vulnerability Insight
The flaws are caused by unspecified errors, that can be exploited to execute arbitrary code or cause a denial of service.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities (Linux)

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.801630
Version used: $Revision: 5263 $

References

CVE: CVE-2010-3636, CVE-2010-3637, CVE-2010-3638, CVE-2010-3639, CVE-2010-3640, ↪CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE ↪-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, CVE-20 ↪10-3652
BID:44669
Other:
URL:http://secunia.com/advisories/41917
URL:http://www.adobe.com/support/security/bulletins/apsb10-26.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities (Linux) - Feb12

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to execute arbitrary code in the context of the affected application or cause a denial of service condition. Impact Level: Application.

Solution

Upgrade to Adobe Flash Player version 10.3.183.15 or 11.1.102.62 or later, For updates refer to http://www.adobe.com/downloads/

Affected Software/OS

Adobe Flash Player version before 10.3.183.15 Adobe Flash Player version 11.x through 11.1.102.55 on Linux

Vulnerability Insight

The flaws are due to, - A memory corruption error in ActiveX control - A type confusion memory corruption error - An unspecified error related to MP4 parsing - Many unspecified erros which allows to bypass certain security restrictions - Improper validation of user supplied input which allows attackers to execute arbitrary HTML and script code in a user's browser session

Vulnerability Detection Method

Details:Adobe Flash Player Multiple Vulnerabilities (Linux) - Feb12
OID:1.3.6.1.4.1.25623.1.0.802804
Version used: $Revision: 5958 $

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2012-0752, CVE-2012-0753, CVE-2012-0754, CVE-2012-0757, CVE-2012-0756,
↪CVE-2012-0767
BID:52032, 52033, 52034, 51999, 52036, 52040
Other:
URL:http://secunia.com/advisories/48033
URL:http://securitytracker.com/id/1026694
URL:http://www.securelist.com/en/advisories/48033
URL:http://www.adobe.com/support/security/bulletins/apsb12-03.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities (Linux) - Feb12

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code in the context of the affected application or cause a denial of service condition. Impact Level: Application.

Solution
Upgrade to Adobe Flash Player version 10.3.183.15 or 11.1.102.62 or later, For updates refer to http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version before 10.3.183.15 Adobe Flash Player version 11.x through 11.1.102.55 on Linux

Vulnerability Insight
The flaws are due to, - A memory corruption error in ActiveX control - A type confusion memory corruption error - An unspecified error related to MP4 parsing - Many unspecified erros which allows to bypass certain security restrictions - Improper validation of user supplied input which allows attackers to execute arbitrary HTML and script code in a user's browser session

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities (Linux) - Feb12
OID:1.3.6.1.4.1.25623.1.0.802804
Version used: $Revision: 5958 $

References
CVE: CVE-2012-0752, CVE-2012-0753, CVE-2012-0754, CVE-2012-0757, CVE-2012-0756,
↪CVE-2012-0767
BID:52032, 52033, 52034, 51999, 52036, 52040
Other:

... continues on next page ...

... continued from previous page ...

URL:http://secunia.com/advisories/48033
URL:http://securitytracker.com/id/1026694
URL:http://www.securelist.com/en/advisories/48033
URL:http://www.adobe.com/support/security/bulletins/apsb12-03.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities (Linux) - Mar12

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain sensitive information or execute arbitrary code in the context of the affected application or cause a denial of service condition. Impact Level: System/Application

Solution
Upgrade to Adobe Flash Player version 10.3.183.16 or 11.1.102.63 or later, For updates refer to http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version before 10.3.183.16 on Linux Adobe Flash Player version 11.x before 11.1.102.63 on Linux

Vulnerability Insight
The flaws are due to an integer errors and Unspecified error in Matrix3D component.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities (Linux) - Mar12
OID:1.3.6.1.4.1.25623.1.0.802810
Version used: $Revision: 5931 $

References
CVE: CVE-2012-0769, CVE-2012-0768
BID:52299, 52297
Other:
URL:http://secunia.com/advisories/48281/
URL:http://www.adobe.com/support/security/bulletins/apsb12-05.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities (Linux) - Mar12

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain sensitive information or execute arbitrary code in the context of the affected application or cause a denial of service condition. Impact Level: System/Application

Solution
Upgrade to Adobe Flash Player version 10.3.183.16 or 11.1.102.63 or later, For updates refer to http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version before 10.3.183.16 on Linux Adobe Flash Player version 11.x before 11.1.102.63 on Linux

Vulnerability Insight
The flaws are due to an integer errors and Unspecified error in Matrix3D component.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities (Linux) - Mar12
OID:1.3.6.1.4.1.25623.1.0.802810
Version used: $Revision: 5931 $

References
CVE: CVE-2012-0769, CVE-2012-0768
BID:52299, 52297
Other:
URL:http://secunia.com/advisories/48281/
URL:http://www.adobe.com/support/security/bulletins/apsb12-05.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 Apr15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 11.2.202.457

Impact
Successful exploitation will allow remote attackers to cause denial of service, execute arbitrary code, bypass the ASLR protection mechanism via unspecified vectors and allow local users to gain privileges .
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.457 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.457 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - Multiple unspecified use-after-free errors. - Multiple unspecified double free vulnerabilities. - An overflow condition that is triggered as user-supplied input is not properly validated. - Improper restriction of discovery of memory addresses.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities - 01 Apr15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805466
Version used: $Revision: 3496 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-3044, CVE-2015-3043, CVE-2015-3042, CVE-2015-3041, CVE-2015-3040,
↪CVE-2015-3039, CVE-2015-3038, CVE-2015-0360, CVE-2015-0359, CVE-2015-0357, CVE
↪-2015-0356, CVE-2015-0355, CVE-2015-0354, CVE-2015-0353, CVE-2015-0352, CVE-20
↪15-0351, CVE-2015-0350, CVE-2015-0349, CVE-2015-0348, CVE-2015-0347, CVE-2015-
↪0346, CVE-2015-0358
BID:74065, 74062, 74068, 74064, 74067, 74066, 74069
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb15-06.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 Apr15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.457

Impact
Successful exploitation will allow remote attackers to cause denial of service, execute arbitrary code, bypass the ASLR protection mechanism via unspecified vectors and allow local users to gain privileges .
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.457 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.457 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - Multiple unspecified use-after-free errors. - Multiple unspecified double free vulnerabilities. - An overflow condition that is triggered as user-supplied input is not properly validated. - Improper restriction of discovery of memory addresses.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities - 01 Apr15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805466
Version used: $Revision: 3496 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
. . . continues on next page . . .

... continued from previous page ...

CVE: CVE-2015-3044, CVE-2015-3043, CVE-2015-3042, CVE-2015-3041, CVE-2015-3040,
↪CVE-2015-3039, CVE-2015-3038, CVE-2015-0360, CVE-2015-0359, CVE-2015-0357, CVE
↪-2015-0356, CVE-2015-0355, CVE-2015-0354, CVE-2015-0353, CVE-2015-0352, CVE-20
↪15-0351, CVE-2015-0350, CVE-2015-0349, CVE-2015-0348, CVE-2015-0347, CVE-2015-
↪0346, CVE-2015-0358
BID:74065, 74062, 74068, 74064, 74067, 74066, 74069
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb15-06.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 Feb14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to, disclose potentially sensitive information and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.341 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.341 on Linux

Vulnerability Insight
Flaw is due to multiple unspecified and a double free error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities - 01 Feb14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.903340
Version used: $Revision: 3555 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0498, CVE-2014-0499, CVE-2014-0502
BID:65704, 65703, 65702
Other:
URL:http://secunia.com/advisories/57057
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-07.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 Feb14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to, disclose potentially sensitive information and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.341 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.341 on Linux

Vulnerability Insight
Flaw is due to multiple unspecified and a double free error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

... continues on next page ...

... continued from previous page ...

Details:Adobe Flash Player Multiple Vulnerabilities - 01 Feb14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.903340
Version used: $Revision: 3555 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0498, CVE-2014-0499, CVE-2014-0502
BID:65704, 65703, 65702
Other:
URL:http://secunia.com/advisories/57057
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-07.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 Mar15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 11.2.202.451

Impact
Successful exploitation will allow remote attackers to cause denial of service execute arbitrary code, bypass intended file-upload restrictions or have other unspecified impacts.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.451 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.451 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple flaws exists due to, - Multiple unspecified use-after-free errors. - Multiple unspecified errors due to improper validation of user-supplied input. - Multiple unspecified type confusion errors. - Integer overflow in adobe Flash Player.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities - 01 Mar15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805493
Version used: `$Revision: 3496 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-0342, CVE-2015-0341, CVE-2015-0340, CVE-2015-0339, CVE-2015-0338,
↪CVE-2015-0337, CVE-2015-0336, CVE-2015-0335, CVE-2015-0334, CVE-2015-0333, CVE
↪-2015-0332
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-05.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 Mar15 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 9.0.31.0
Fixed version:     11.2.202.451
```

Impact
Successful exploitation will allow remote attackers to cause denial of service execute arbitrary code, bypass intended file-upload restrictions or have other unspecified impacts.
Impact Level: System/Application.

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to Adobe Flash Player version 11.2.202.451 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.451 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - Multiple unspecified use-after-free errors. - Multiple unspecified errors due to improper validation of user-supplied input. - Multiple unspecified type confusion errors. - Integer overflow in adobe Flash Player.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities - 01 Mar15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805493
Version used: `$Revision: 3496 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-0342, CVE-2015-0341, CVE-2015-0340, CVE-2015-0339, CVE-2015-0338,
↪CVE-2015-0337, CVE-2015-0336, CVE-2015-0335, CVE-2015-0334, CVE-2015-0333, CVE
↪-2015-0332
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-05.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 May15 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 7.0.63.0
Fixed version:     11.2.202.460
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow a context-dependent attacker to corrupt memory and potentially execute arbitrary code, bypass security restrictions and gain access to sensitive information, bypass protected mode, bypass validation mechanisms and write arbitrary data, bypass the sandbox when chained with another vulnerability, bypass ASLR protection mechanisms.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.460 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player versions before 11.2.202.460 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - Improper validation of user supplied input. - A flaw in the Broker that is due to the BrokerCreateFile method not properly sanitizing user input. - An integer overflow condition that is triggered as user-supplied input is not properly validated. - An overflow condition that is triggered as user-supplied input is not properly validated. - Multiple unspecified memory disclosure flaws in Adobe Flash Player. - Multiple unspecified type confusion flaws in Adobe Flash Player. - Multiple unspecified flaws in Adobe Flash Player. - A a use-after-free error Adobe Flash Player. - An unspecified TOCTOU flaw in Adobe Flash Player.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities - 01 May15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805619
Version used: `$Revision: 3496 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-3077, CVE-2015-3078, CVE-2015-3079, CVE-2015-3080, CVE-2015-3081,
↪CVE-2015-3082, CVE-2015-3083, CVE-2015-3084, CVE-2015-3085, CVE-2015-3086, CVE
↪-2015-3087, CVE-2015-3088, CVE-2015-3089, CVE-2015-3090, CVE-2015-3091, CVE-20
↪15-3092, CVE-2015-3093
BID:74614, 74605, 74612, 74608, 74613, 74610, 74616, 74609, 74617
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-09.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 May15 (Linux)

Product detection result
`cpe:/a:adobe:flash_player:9.0.31.0`
`Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2`
`↪5623.1.0.800032)`

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 9.0.31.0`
`Fixed version: 11.2.202.460`

Impact
Successful exploitation will allow a context-dependent attacker to corrupt memory and potentially execute arbitrary code, bypass security restrictions and gain access to sensitive information, bypass protected mode, bypass validation mechanisms and write arbitrary data, bypass the sandbox when chained with another vulnerability, bypass ASLR protection mechanisms.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.460 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player versions before 11.2.202.460 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - Improper validation of user supplied input. - A flaw in the Broker that is due to the BrokerCreateFile method not properly sanitizing user input. - An integer overflow condition that is triggered as user-supplied input is not properly validated. - An overflow condition that is triggered as user-supplied input is not properly validated. - Multiple unspecified memory disclosure flaws in Adobe Flash Player. - Multiple unspecified type confusion flaws in Adobe Flash Player. - Multiple unspecified flaws in Adobe Flash Player. - A a use-after-free error Adobe Flash Player. - An unspecified TOCTOU flaw in Adobe Flash Player.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities - 01 May15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805619
Version used: `$Revision: 3496 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`

. . . continues on next page . . .

... continued from previous page ...

Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References

```
CVE: CVE-2015-3077, CVE-2015-3078, CVE-2015-3079, CVE-2015-3080, CVE-2015-3081,
↪CVE-2015-3082, CVE-2015-3083, CVE-2015-3084, CVE-2015-3085, CVE-2015-3086, CVE
↪-2015-3087, CVE-2015-3088, CVE-2015-3089, CVE-2015-3090, CVE-2015-3091, CVE-20
↪15-3092, CVE-2015-3093
BID:74614, 74605, 74612, 74608, 74613, 74610, 74616, 74609, 74617
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-09.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 Oct15 (Linux)

Product detection result

```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.0.63.0
Fixed version:     11.2.202.535
```

Impact

Successful exploitation will allow attackers to obtain sensitive information, execute arbitrary code or cause a denial of service and have other unspecified impacts.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.535 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player before version 11.2.202.535 on Linux.

Vulnerability Insight

Multiple flaws exists due to, - Improper implementation of the Flash broker API. - Multiple memory corruption errors. - An use-after-free error. - An error in same origin policy. - A buffer overflow error.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities - 01 Oct15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.806095
Version used: $Revision: 2582 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-5569, CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7628,
↪CVE-2015-7629, CVE-2015-7630, CVE-2015-7631, CVE-2015-7632, CVE-2015-7633, CVE
↪-2015-7634, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-20
↪15-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, CVE-2015-
↪7644
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb15-25.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - 01 Oct15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.535

Impact
Successful exploitation will allow attackers to obtain sensitive information, execute arbitrary code or cause a denial of service and have other unspecified impacts.
Impact Level: System/Application.

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to Adobe Flash Player version 11.2.202.535 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.535 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - Improper implementation of the Flash broker API. - Multiple memory corruption errors. - An use-after-free error. - An error in same origin policy. - A buffer overflow error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities - 01 Oct15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806095
Version used: `$Revision: 2582 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-5569, CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7628,
↪CVE-2015-7629, CVE-2015-7630, CVE-2015-7631, CVE-2015-7632, CVE-2015-7633, CVE
↪-2015-7634, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-20
↪15-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, CVE-2015-
↪7644
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-25.html
```

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities - 02 Apr14 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow attackers to conduct cross-site scripting attacks, bypass certain security restrictions, and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.350 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.350 on Linux

Vulnerability Insight
Multiple flaws are due to, - An error related to regular expressions in ActionScript. - An use-after-free error and multiple unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities - 02 Apr14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804539
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2014-0507, CVE-2014-0508, CVE-2014-0509
BID:66701, 66699, 66703
Other:
  URL:http://secunia.com/advisories/57661
   URL:http://helpx.adobe.com/security/products/flash-player/apsb14-09.html
```

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities - 02 Apr14 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to conduct cross-site scripting attacks, bypass certain security restrictions, and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.350 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.350 on Linux

Vulnerability Insight
Multiple flaws are due to, - An error related to regular expressions in ActionScript. - An use-after-free error and multiple unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities - 02 Apr14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804539
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2014-0507, CVE-2014-0508, CVE-2014-0509`
`BID:66701, 66699, 66703`
`Other:`
`URL:http://secunia.com/advisories/57661`
`URL:http://helpx.adobe.com/security/products/flash-player/apsb14-09.html`

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - December12 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or denial of service.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.48 or 11.2.202.258 or later, For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version before 10.3.183.48, 11.x before 11.2.202.258 on Linux

Vulnerability Insight
Multiple unspecified errors and integer overflow exists that could lead to code execution.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities - December12 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803076
Version used: `$Revision: 5963 $`

References
```
CVE: CVE-2012-5676, CVE-2012-5677, CVE-2012-5678
BID:56892, 56896, 56898
Other:
  URL:http://secunia.com/advisories/51560/
   URL:http://securitytracker.com/id?1027854
   URL:http://technet.microsoft.com/en-us/security/advisory/2755801
   URL:http://www.adobe.com/support/security/bulletins/apsb12-27.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - December12 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or denial of service.
Impact Level: System/Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.48 or 11.2.202.258 or later, For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version before 10.3.183.48, 11.x before 11.2.202.258 on Linux

Vulnerability Insight
Multiple unspecified errors and integer overflow exists that could lead to code execution.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities - December12 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803076
Version used: `$Revision: 5963 $`

References
```
CVE: CVE-2012-5676, CVE-2012-5677, CVE-2012-5678
BID:56892, 56896, 56898
Other:
  URL:http://secunia.com/advisories/51560/
   URL:http://securitytracker.com/id?1027854
   URL:http://technet.microsoft.com/en-us/security/advisory/2755801
   URL:http://www.adobe.com/support/security/bulletins/apsb12-27.html
```

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities - Mar09 (Linux)

Summary
This host is installed with Adobe Products and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause remote code execution, compromise system privileges or may cause exposure of sensitive information. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to version Adobe Flash Player 9.0.159.0 or 10.0.22.87 http://get.adobe.com/flashplayer
Update to version 1.5.1 for Adobe AIR http://get.adobe.com/air

Affected Software/OS

... continues on next page ...

. . . continued from previous page . . .

Adobe AIR version prior to 1.5.1 Adobe Flash Player 9 version prior to 9.0.159.0 Adobe Flash Player 10 version prior to 10.0.22.87

Vulnerability Insight
- Error while processing multiple references to an unspecified object which can be exploited by tricking the user to access a malicious crafted SWF file. - Input validation error in the processing of SWF file. - Error while displaying the mouse pointer on Windows which may cause 'Clickjacking' attacks. - Error in the Linux Flash Player binaries which can cause disclosure of sensitive information.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities - Mar09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800360
Version used: `$Revision: 4865 $`

References
`CVE: CVE-2009-0114, CVE-2009-0519, CVE-2009-0520, CVE-2009-0521, CVE-2009-0522`
`BID:33890`
`Other:`
`URL:http://secunia.com/advisories/34012`
`URL:http://www.adobe.com/support/security/bulletins/apsb09-01.html`

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities - Mar09 (Linux)

Summary
This host is installed with Adobe Products and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause remote code execution, compromise system privileges or may cause exposure of sensitive information. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to version Adobe Flash Player 9.0.159.0 or 10.0.22.87 http://get.adobe.com/flashplayer
Update to version 1.5.1 for Adobe AIR http://get.adobe.com/air

Affected Software/OS
Adobe AIR version prior to 1.5.1 Adobe Flash Player 9 version prior to 9.0.159.0 Adobe Flash Player 10 version prior to 10.0.22.87

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

- Error while processing multiple references to an unspecified object which can be exploited by tricking the user to access a malicious crafted SWF file. - Input validation error in the processing of SWF file. - Error while displaying the mouse pointer on Windows which may cause 'Clickjacking' attacks. - Error in the Linux Flash Player binaries which can cause disclosure of sensitive information.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities - Mar09 (Linux)
OID:1.3.6.1.4.1.25623.1.0.800360
Version used: $Revision: 4865 $

References
CVE: CVE-2009-0114, CVE-2009-0519, CVE-2009-0520, CVE-2009-0521, CVE-2009-0522
BID:33890
Other:
URL:http://secunia.com/advisories/34012
URL:http://www.adobe.com/support/security/bulletins/apsb09-01.html

High (CVSS: 7.5)
NVT: Adobe Flash Player Multiple Vulnerabilities - May14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to bypass certain security restrictions and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.359 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.359 on Linux

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple flaws are due to an use-after free error when handling display objects and multiple unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities - May14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804591
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2014-0516, CVE-2014-0517, CVE-2014-0518, CVE-2014-0519, CVE-2014-0520
BID:67361, 67364, 67371, 67373, 67372
Other:
  URL:http://secunia.com/advisories/58074
   URL:http://helpx.adobe.com/security/products/flash-player/apsb14-14.html
```

High (CVSS: 7.5)
NVT: Adobe Flash Player Multiple Vulnerabilities - May14 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to bypass certain security restrictions and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Update to Adobe Flash Player version 11.2.202.359 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.359 on Linux

Vulnerability Insight
Multiple flaws are due to an use-after free error when handling display objects and multiple unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities - May14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804591
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2014-0516, CVE-2014-0517, CVE-2014-0518, CVE-2014-0519, CVE-2014-0520
BID:67361, 67364, 67371, 67373, 67372
Other:
  URL:http://secunia.com/advisories/58074
   URL:http://helpx.adobe.com/security/products/flash-player/apsb14-14.html
```

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities - Nov08 (Linux)

Summary
This host has Adobe Flash Player installed and is prone to multiple security bypass vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful attack could allow malicious people to bypass certain security restrictions or manipulate certain data. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player 9.0.151.0 or 10.0.12.36, http://www.adobe.com/downloads/

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Adobe Flash Player 9.0.124.0 and earlier on Linux.

Vulnerability Insight
Multiple flaws are reported in Adobe Flash Player, for more information refer, http://www.adobe.com/support/security/bulletins/apsb08-20.html http://www.adobe.com/support/security/bulletins/apsb08-22.html

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities - Nov08 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800055
Version used: `$Revision: 4218 $`

References
```
CVE: CVE-2008-4818, CVE-2008-4819, CVE-2008-4820, CVE-2008-4821, CVE-2008-4822,
↪CVE-2008-4823, CVE-2008-4824, CVE-2008-5361, CVE-2008-5362, CVE-2008-5363
BID:32129
Other:
  URL:http://www.adobe.com/support/security/bulletins/apsb08-20.html
   URL:http://www.adobe.com/support/security/bulletins/apsb08-22.html
```

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities - Nov08 (Linux)

Summary
This host has Adobe Flash Player installed and is prone to multiple security bypass vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful attack could allow malicious people to bypass certain security restrictions or manipulate certain data. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player 9.0.151.0 or 10.0.12.36, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player 9.0.124.0 and earlier on Linux.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws are reported in Adobe Flash Player, for more information refer, http://www.adobe.com/support/security/bulletins/apsb08-20.html http://www.adobe.com/support/security/bulletins/apsb08-22.html

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities - Nov08 (Linux)
OID:1.3.6.1.4.1.25623.1.0.800055
Version used: $Revision: 4218 $

References
CVE: CVE-2008-4818, CVE-2008-4819, CVE-2008-4820, CVE-2008-4821, CVE-2008-4822,
↪CVE-2008-4823, CVE-2008-4824, CVE-2008-5361, CVE-2008-5362, CVE-2008-5363
BID:32129
Other:
URL:http://www.adobe.com/support/security/bulletins/apsb08-20.html
URL:http://www.adobe.com/support/security/bulletins/apsb08-22.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - November 11 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: Application/System

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.11 or 11.1.102.55 or later For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version prior to 10.3.183.11 and 11.x through 11.0.1.152 on Linux

Vulnerability Insight
The flaws are due to memory corruption, heap corruption, buffer overflow, stack overflow errors that could lead to code execution.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities - November 11 (Linux)
OID:1.3.6.1.4.1.25623.1.0.902752
Version used: $Revision: 3114 $

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2011-2445, CVE-2011-2450, CVE-2011-2451, CVE-2011-2452, CVE-2011-2453,
↪CVE-2011-2454, CVE-2011-2455, CVE-2011-2456, CVE-2011-2457, CVE-2011-2458, CVE
↪-2011-2459, CVE-2011-2460
BID:50625, 50619, 50623, 50622, 50618, 50626, 50627, 50624, 50621, 50629, 50620,
↪ 50628
Other:
URL:http://secunia.com/advisories/46818/
URL:http://www.adobe.com/support/security/bulletins/apsb11-28.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - November 11 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: Application/System

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.11 or 11.1.102.55 or later For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version prior to 10.3.183.11 and 11.x through 11.0.1.152 on Linux

Vulnerability Insight
The flaws are due to memory corruption, heap corruption, buffer overflow, stack overflow errors that could lead to code execution.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities - November 11 (Linux)
OID:1.3.6.1.4.1.25623.1.0.902752
Version used: $Revision: 3114 $

References
CVE: CVE-2011-2445, CVE-2011-2450, CVE-2011-2451, CVE-2011-2452, CVE-2011-2453,
↪CVE-2011-2454, CVE-2011-2455, CVE-2011-2456, CVE-2011-2457, CVE-2011-2458, CVE
↪-2011-2459, CVE-2011-2460
BID:50625, 50619, 50623, 50622, 50618, 50626, 50627, 50624, 50621, 50629, 50620,

... continues on next page ...

... continued from previous page ...

↪ 50628
Other:
URL:http://secunia.com/advisories/46818/
URL:http://www.adobe.com/support/security/bulletins/apsb11-28.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - November12 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain sensitive information or execute arbitrary code in the context of the affected application. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.43 or 11.2.202.251 or later, For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version before 10.3.183.43, 11.x before 11.2.202.251 on Linux

Vulnerability Insight
Multiple unspecified errors exists due to memory corruption, buffer overflow that could lead to code execution.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities - November12 (Linux)
OID:1.3.6.1.4.1.25623.1.0.803046
Version used: $Revision: 5940 $

References
CVE: CVE-2012-5274, CVE-2012-5275, CVE-2012-5276, CVE-2012-5277, CVE-2012-5278,
↪CVE-2012-5279, CVE-2012-5280
BID:56412
Other:
URL:http://secunia.com/advisories/51213
URL:http://www.adobe.com/support/security/bulletins/apsb12-24.html

... continues on next page ...

... continued from previous page ...

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - November12 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain sensitive information or execute arbitrary code in the context of the affected application. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.43 or 11.2.202.251 or later, For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version before 10.3.183.43, 11.x before 11.2.202.251 on Linux

Vulnerability Insight
Multiple unspecified errors exists due to memory corruption, buffer overflow that could lead to code execution.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities - November12 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803046
Version used: `$Revision: 5940 $`

References
```
CVE: CVE-2012-5274, CVE-2012-5275, CVE-2012-5276, CVE-2012-5277, CVE-2012-5278,
↪CVE-2012-5279, CVE-2012-5280
BID:56412
Other:
  URL:http://secunia.com/advisories/51213
   URL:http://www.adobe.com/support/security/bulletins/apsb12-24.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - Oct12 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code on the target system or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.29 or 11.2.202.243 or later, For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version before 10.3.183.29, 11.x before 11.2.202.243 on Linux

Vulnerability Insight
The flaws are due to memory corruption, buffer overflow errors that could lead to code execution.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities - Oct12 (Linux)
OID:1.3.6.1.4.1.25623.1.0.802988
Version used: $Revision: 5940 $

References
```
CVE: CVE-2012-5248, CVE-2012-5249, CVE-2012-5250, CVE-2012-5251, CVE-2012-5252,
↪CVE-2012-5253, CVE-2012-5254, CVE-2012-5255, CVE-2012-5256, CVE-2012-5257, CVE
↪-2012-5258, CVE-2012-5259, CVE-2012-5260, CVE-2012-5261, CVE-2012-5262, CVE-20
↪12-5263, CVE-2012-5264, CVE-2012-5265, CVE-2012-5266, CVE-2012-5267, CVE-2012-
↪5268, CVE-2012-5269, CVE-2012-5270, CVE-2012-5271, CVE-2012-5272, CVE-2012-567
↪3, CVE-2012-5285, CVE-2012-5286, CVE-2012-5287
BID:55827, 56374, 56375, 56376, 56377
Other:
  URL:http://secunia.com/advisories/50876/
   URL:http://www.adobe.com/support/security/bulletins/apsb12-22.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - Oct12 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to execute arbitrary code on the target system or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.29 or 11.2.202.243 or later, For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version before 10.3.183.29, 11.x before 11.2.202.243 on Linux

Vulnerability Insight
The flaws are due to memory corruption, buffer overflow errors that could lead to code execution.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities - Oct12 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.802988
Version used: `$Revision: 5940 $`

References
```
CVE: CVE-2012-5248, CVE-2012-5249, CVE-2012-5250, CVE-2012-5251, CVE-2012-5252,
↪CVE-2012-5253, CVE-2012-5254, CVE-2012-5255, CVE-2012-5256, CVE-2012-5257, CVE
↪-2012-5258, CVE-2012-5259, CVE-2012-5260, CVE-2012-5261, CVE-2012-5262, CVE-20
↪12-5263, CVE-2012-5264, CVE-2012-5265, CVE-2012-5266, CVE-2012-5267, CVE-2012-
↪5268, CVE-2012-5269, CVE-2012-5270, CVE-2012-5271, CVE-2012-5272, CVE-2012-567
↪3, CVE-2012-5285, CVE-2012-5286, CVE-2012-5287
BID:55827, 56374, 56375, 56376, 56377
Other:
  URL:http://secunia.com/advisories/50876/
   URL:http://www.adobe.com/support/security/bulletins/apsb12-22.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - Sep12 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code on the target system or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: System/Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.23 or 11.4.402.265 or later For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version before 10.3.183.23, 11.x before 11.2.202.238 on Linux

Vulnerability Insight
- Multiple errors due to memory corruption, integer overflow that could lead to code execution.
- A logic error due to improper handling of multiple dialogs in Firefox allows attackers to crash the application.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities - Sep12 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803024
Version used: `$Revision: 5988 $`

References
```
CVE: CVE-2012-4163, CVE-2012-4164, CVE-2012-4165, CVE-2012-4166, CVE-2012-4167,
↪CVE-2012-4168, CVE-2012-4171, CVE-2012-5054
BID:55136, 55365
Other:
  URL:http://secunia.com/advisories/50354/
   URL:http://www.adobe.com/support/security/bulletins/apsb12-19.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities - Sep12 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code on the target system or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.23 or 11.4.402.265 or later For updates refer to http://get.adobe.com/flashplayer/

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Adobe Flash Player version before 10.3.183.23, 11.x before 11.2.202.238 on Linux

Vulnerability Insight
- Multiple errors due to memory corruption, integer overflow that could lead to code execution.
- A logic error due to improper handling of multiple dialogs in Firefox allows attackers to crash the application.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities - Sep12 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803024
Version used: `$Revision: 5988 $`

References
```
CVE: CVE-2012-4163, CVE-2012-4164, CVE-2012-4165, CVE-2012-4166, CVE-2012-4167,
↪CVE-2012-4168, CVE-2012-4171, CVE-2012-5054
BID:55136, 55365
Other:
  URL:http://secunia.com/advisories/50354/
   URL:http://www.adobe.com/support/security/bulletins/apsb12-19.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 April 13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause denial-of-service condition. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to version 10.3.183.68 or 11.2.202.275, For updates refer to http://www.adobe.com/products/flash.html

Affected Software/OS
Adobe Flash Player 10.3.183.67 and earlier, and 11.x to 11.2.202.274 on Linux

Vulnerability Insight
Multiple flaws due to, - Heap based overflow via unspecified vectors. - Integer overflow via unspecified vectors. - Use-after-free errors.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details:Adobe Flash Player Multiple Vulnerabilities -01 April 13 (Linux)
OID:1.3.6.1.4.1.25623.1.0.803375
Version used: $Revision: 2923 $

References
CVE: CVE-2013-1375, CVE-2013-1371, CVE-2013-0650, CVE-2013-0646
BID:58439, 58438, 58440, 58436
Other:
URL:http://secunia.com/advisories/52590
URL:http://www.adobe.com/support/security/bulletins/apsb13-09.html
URL:https://www.cert.be/pro/advisories/adobe-flash-player-air-multiple-vulner
↪abilities-2

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 April 13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause denial-of-service condition. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to version 10.3.183.68 or 11.2.202.275, For updates refer to http://www.adobe.com/products/flash.html

Affected Software/OS
Adobe Flash Player 10.3.183.67 and earlier, and 11.x to 11.2.202.274 on Linux

Vulnerability Insight
Multiple flaws due to, - Heap based overflow via unspecified vectors. - Integer overflow via unspecified vectors. - Use-after-free errors.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities -01 April 13 (Linux)
OID:1.3.6.1.4.1.25623.1.0.803375
Version used: $Revision: 2923 $

References
CVE: CVE-2013-1375, CVE-2013-1371, CVE-2013-0650, CVE-2013-0646
BID:58439, 58438, 58440, 58436

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://secunia.com/advisories/52590
   URL:http://www.adobe.com/support/security/bulletins/apsb13-09.html
   URL:https://www.cert.be/pro/advisories/adobe-flash-player-air-multiple-vulner
↪abilities-2
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 Aug15 (Linux)

Product detection result

```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.0.63.0
Fixed version:     11.2.202.508
```

Impact

Successful exploitation will allow remote attackers to conduct denial of service attack, execute arbitrary code in the context of the affected user and possibly have other unspecified impact.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.508 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player before version 11.2.202.508 on Linux.

Vulnerability Insight

Multiple flaws exist due to multiple type confusion errors, a vector-length corruption error, multiple use-after-free errors, multiple heap buffer overflow errors, multiple buffer overflow errors, multiple memory corruption errors and an integer overflow error.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities -01 Aug15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805956
Version used: `$Revision: 2582 $`

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-5124, CVE-2015-5125, CVE-2015-5127, CVE-2015-5129, CVE-2015-5130, ↪CVE-2015-5131, CVE-2015-5132, CVE-2015-5133, CVE-2015-5134, CVE-2015-5539, CVE ↪-2015-5540, CVE-2015-5541, CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-20 ↪15-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5550, CVE-2015-5551, CVE-2015- ↪5552, CVE-2015-5553, CVE-2015-5554, CVE-2015-5555, CVE-2015-5556, CVE-2015-555 ↪7, CVE-2015-5558, CVE-2015-5559, CVE-2015-5560, CVE-2015-5561, CVE-2015-5562, ↪CVE-2015-5563, CVE-2015-5564, CVE-2015-5565, CVE-2015-5566
BID:75959, 76291, 76282, 76282, 76283, 76283, 76289, 76288, 76287
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb15-19.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 Aug15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2 ↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.508

Impact
Successful exploitation will allow remote attackers to conduct denial of service attack, execute arbitrary code in the context of the affected user and possibly have other unspecified impact.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.508 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.508 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple flaws exist due to multiple type confusion errors, a vector-length corruption error, multiple use-after-free errors, multiple heap buffer overflow errors, multiple buffer overflow errors, multiple memory corruption errors and an integer overflow error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities -01 Aug15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805956
Version used: $Revision: 2582 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-5124, CVE-2015-5125, CVE-2015-5127, CVE-2015-5129, CVE-2015-5130,
↪CVE-2015-5131, CVE-2015-5132, CVE-2015-5133, CVE-2015-5134, CVE-2015-5539, CVE
↪-2015-5540, CVE-2015-5541, CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-20
↪15-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5550, CVE-2015-5551, CVE-2015-
↪5552, CVE-2015-5553, CVE-2015-5554, CVE-2015-5555, CVE-2015-5556, CVE-2015-555
↪7, CVE-2015-5558, CVE-2015-5559, CVE-2015-5560, CVE-2015-5561, CVE-2015-5562,
↪CVE-2015-5563, CVE-2015-5564, CVE-2015-5565, CVE-2015-5566
BID:75959, 76291, 76282, 76282, 76283, 76283, 76289, 76288, 76287
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb15-19.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 Dec15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 11.2.202.559

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to bypass execute arbitrary code on the affected system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.559 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.559 on Linux.

Vulnerability Insight
Multiple flaws exist due to, - A type confusion vulnerability. - An integer overflow vulnerability. - Multiple use-after-free vulnerabilities. - Multiple memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities -01 Dec15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807019
Version used: `$Revision: 2582 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-8459, CVE-2015-8460, CVE-2015-8634, CVE-2015-8635, CVE-2015-8636,
↪CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE
↪-2015-8643, CVE-2015-8644, CVE-2015-8645, CVE-2015-8646, CVE-2015-8647, CVE-20
↪15-8648, CVE-2015-8649, CVE-2015-8650, CVE-2015-8651
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-01.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 Dec15 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 9.0.31.0`
`Fixed version: 11.2.202.559`

Impact
Successful exploitation will allow attackers to bypass execute arbitrary code on the affected system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.559 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.559 on Linux.

Vulnerability Insight
Multiple flaws exist due to, - A type confusion vulnerability. - An integer overflow vulnerability. - Multiple use-after-free vulnerabilities. - Multiple memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities -01 Dec15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807019
Version used: `$Revision: 2582 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-8459, CVE-2015-8460, CVE-2015-8634, CVE-2015-8635, CVE-2015-8636,
↪CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE
↪-2015-8643, CVE-2015-8644, CVE-2015-8645, CVE-2015-8646, CVE-2015-8647, CVE-20
↪15-8648, CVE-2015-8649, CVE-2015-8650, CVE-2015-8651
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-01.html
```

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 Feb13 (Linux)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause buffer overflow, remote code execution, and corrupt system memory. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to version 11.2.202.262 or later, For updates refer to http://www.adobe.com/products/flash.html

Affected Software/OS
Adobe Flash Player prior to 10.3.183.51 and 11.x prior to 11.2.202.262 on Linux

Vulnerability Insight
Error while processing multiple references to an unspecified object which can be exploited by tricking the user to accessing a malicious crafted SWF file.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities -01 Feb13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803406
Version used: `$Revision: 2923 $`

References
```
CVE: CVE-2013-0633, CVE-2013-0634
BID:57787, 57788
Other:
  URL:http://secunia.com/advisories/52116
   URL:http://xforce.iss.net/xforce/xfdb/81866
   URL:http://www.adobe.com/support/security/bulletins/apsb13-04.html
```

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 Feb13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to cause buffer overflow, remote code execution, and corrupt system memory. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to version 11.2.202.262 or later, For updates refer to http://www.adobe.com/products/flash.html

Affected Software/OS
Adobe Flash Player prior to 10.3.183.51 and 11.x prior to 11.2.202.262 on Linux

Vulnerability Insight
Error while processing multiple references to an unspecified object which can be exploited by tricking the user to accessing a malicious crafted SWF file.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities -01 Feb13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803406
Version used: `$Revision: 2923 $`

References
```
CVE: CVE-2013-0633, CVE-2013-0634
BID:57787, 57788
Other:
  URL:http://secunia.com/advisories/52116
   URL:http://xforce.iss.net/xforce/xfdb/81866
   URL:http://www.adobe.com/support/security/bulletins/apsb13-04.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 Feb16 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 7.0.63.0
Fixed version:     11.2.202.569
```

Impact
Successful exploitation will potentially allow an attacker to take control of the affected system, which could lead to code execution.

... continues on next page ...

... continued from previous page ...

Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.569 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.569 on Linux.

Vulnerability Insight
Multiple flaws exist due to, - Multiple memory corruption vulnerabilities - Multiple use-after-free vulnerabilities - A heap buffer overflow vulnerability - A type confusion vulnerability.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities -01 Feb16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806867
Version used: `$Revision: 5527 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968,
↪CVE-2016-0969, CVE-2016-0970, CVE-2016-0971, CVE-2016-0972, CVE-2016-0973, CVE
↪-2016-0974, CVE-2016-0975, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-20
↪16-0979, CVE-2016-0980, CVE-2016-0981, CVE-2016-0982, CVE-2016-0983, CVE-2016-
↪0984, CVE-2016-0985
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-04.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 Feb16 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.569

Impact
Successful exploitation will potentially allow an attacker to take control of the affected system, which could lead to code execution.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.569 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.569 on Linux.

Vulnerability Insight
Multiple flaws exist due to, - Multiple memory corruption vulnerabilities - Multiple use-after-free vulnerabilities - A heap buffer overflow vulnerability - A type confusion vulnerability.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities -01 Feb16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.806867
Version used: $Revision: 5527 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968,
↪CVE-2016-0969, CVE-2016-0970, CVE-2016-0971, CVE-2016-0972, CVE-2016-0973, CVE
↪-2016-0974, CVE-2016-0975, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-20
↪16-0979, CVE-2016-0980, CVE-2016-0981, CVE-2016-0982, CVE-2016-0983, CVE-2016-
↪0984, CVE-2016-0985
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb16-04.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 July15 (Linux)

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 11.2.202.491

Impact
Successful exploitation will allow remote attackers to conduct denial of service attack and potentially execute arbitrary code in the context of the affected user.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.491 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version 11.2.202.481 and prior on Linux.

Vulnerability Insight
Multiple flaws exist due to, - An use-after-free error triggered by freeing a TextLine object within the 'valueOf' function of a custom class when setting the TextLine's opaqueBackground. - An unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities -01 July15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805919
Version used: $Revision: 2582 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-5122, CVE-2015-5123
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsa15-04.html
URL:https://helpx.adobe.com/security/products/flash-player/apsb15-18.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 July15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.491

Impact
Successful exploitation will allow remote attackers to conduct denial of service attack and potentially execute arbitrary code in the context of the affected user.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.491 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version 11.2.202.481 and prior on Linux.

Vulnerability Insight
Multiple flaws exist due to, - An use-after-free error triggered by freeing a TextLine object within the 'valueOf' function of a custom class when setting the TextLine's opaqueBackground. - An unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities -01 July15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805919
Version used: $Revision: 2582 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-5122, CVE-2015-5123

. . . continues on next page . . .

... continued from previous page ...

Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsa15-04.html
URL:https://helpx.adobe.com/security/products/flash-player/apsb15-18.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 March13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause denial-of-service condition. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to version 10.3.183.67 or 11.2.202.273, For updates refer to http://www.adobe.com/products/flash.html

Affected Software/OS
Adobe Flash Player 10.3.183.61 and earlier, and 11.x to 11.2.202.270 on Linux

Vulnerability Insight
Multiple flaws due to, - A flaw in the ExternalInterface ActionScript feature. - Firefox sandbox does not restrict privileges. - Buffer overflow in the Flash Player broker service.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities -01 March13 (Linux)
OID:1.3.6.1.4.1.25623.1.0.803324
Version used: $Revision: 2923 $

References
CVE: CVE-2013-0648, CVE-2013-0643, CVE-2013-0504
BID:58186, 58185, 58184
Other:
URL:http://www.securitytracker.com/id/1028210
URL:http://www.securelist.com/en/advisories/52374
URL:http://www.adobe.com/support/security/bulletins/apsb13-08.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 March13 (Linux)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause denial-of-service condition. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to version 10.3.183.67 or 11.2.202.273, For updates refer to http://www.adobe.com/products/flash.html

Affected Software/OS
Adobe Flash Player 10.3.183.61 and earlier, and 11.x to 11.2.202.270 on Linux

Vulnerability Insight
Multiple flaws due to, - A flaw in the ExternalInterface ActionScript feature. - Firefox sandbox does not restrict privileges. - Buffer overflow in the Flash Player broker service.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities -01 March13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803324
Version used: `$Revision: 2923 $`

References
`CVE: CVE-2013-0648, CVE-2013-0643, CVE-2013-0504`
`BID:58186, 58185, 58184`
`Other:`
`URL:http://www.securitytracker.com/id/1028210`
`URL:http://www.securelist.com/en/advisories/52374`
`URL:http://www.adobe.com/support/security/bulletins/apsb13-08.html`

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 May 13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to execute arbitrary code on the target system or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.86 or 11.2.202.285 or later For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 10.3.183.76 and 11.x before 11.2.202.281 on Linux

Vulnerability Insight
Multiple memory corruption flaws due to improper sanitation of user supplied input via a file.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities -01 May 13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803498
Version used: `$Revision: 3556 $`

References
```
CVE: CVE-2013-3335, CVE-2013-3334, CVE-2013-3333, CVE-2013-3332, CVE-2013-3331,
↪CVE-2013-3330, CVE-2013-3329, CVE-2013-3328, CVE-2013-3327, CVE-2013-3326, CVE
↪-2013-3325, CVE-2013-3324, CVE-2013-2728
BID:59901, 59900, 59899, 59898, 59897, 59896, 59895, 59894, 59893, 59892, 59891,
↪ 59890, 59889
Other:
  URL:http://secunia.com/advisories/53419
   URL:http://www.adobe.com/support/security/bulletins/apsb13-14.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -01 May 13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code on the target system or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Update to Adobe Flash Player version 10.3.183.86 or 11.2.202.285 or later For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 10.3.183.76 and 11.x before 11.2.202.281 on Linux

Vulnerability Insight
Multiple memory corruption flaws due to improper sanitation of user supplied input via a file.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities -01 May 13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803498
Version used: `$Revision: 3556 $`

References
```
CVE: CVE-2013-3335, CVE-2013-3334, CVE-2013-3333, CVE-2013-3332, CVE-2013-3331,
↪CVE-2013-3330, CVE-2013-3329, CVE-2013-3328, CVE-2013-3327, CVE-2013-3326, CVE
↪-2013-3325, CVE-2013-3324, CVE-2013-2728
BID:59901, 59900, 59899, 59898, 59897, 59896, 59895, 59894, 59893, 59892, 59891,
↪ 59890, 59889
Other:
  URL:http://secunia.com/advisories/53419
   URL:http://www.adobe.com/support/security/bulletins/apsb13-14.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -02 April13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause denial-of-service condition. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to version 10.3.183.75 or 11.2.202.280, For updates refer to http://www.adobe.com/products/flash.html

Affected Software/OS
Adobe Flash Player 10.3.183.68 and earlier, and 11.x to 11.2.202.275 on Linux

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws due to, - Error when initializing certain pointer arrays. - Integer overflow error.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities -02 April13 (Linux)
OID:1.3.6.1.4.1.25623.1.0.803383
Version used: $Revision: 2923 $

References
CVE: CVE-2013-1380, CVE-2013-1379, CVE-2013-1378, CVE-2013-2555
BID:58949, 58951, 58947, 58396
Other:
URL:http://www.securelist.com/en/advisories/52931
URL:http://www.adobe.com/support/security/bulletins/apsb13-11.html
URL:http://www.cert.be/pro/advisories/adobe-flash-player-air-multiple-vulnera
↪bilities-3

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -02 April13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause denial-of-service condition. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to version 10.3.183.75 or 11.2.202.280, For updates refer to http://www.adobe.com/products/flash.html

Affected Software/OS
Adobe Flash Player 10.3.183.68 and earlier, and 11.x to 11.2.202.275 on Linux

Vulnerability Insight
Multiple flaws due to, - Error when initializing certain pointer arrays. - Integer overflow error.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities -02 April13 (Linux)
OID:1.3.6.1.4.1.25623.1.0.803383
Version used: $Revision: 2923 $

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2013-1380, CVE-2013-1379, CVE-2013-1378, CVE-2013-2555
BID:58949, 58951, 58947, 58396
Other:
URL:http://www.securelist.com/en/advisories/52931
URL:http://www.adobe.com/support/security/bulletins/apsb13-11.html
URL:http://www.cert.be/pro/advisories/adobe-flash-player-air-multiple-vulnera
↪bilities-3

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -02 Feb13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause buffer overflow, remote code execution and corrupt system memory. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to version 11.2.202.270 or later, For updates refer to http://www.adobe.com/products/flash.html

Affected Software/OS
Adobe Flash Player prior to 10.3.183.61 and 11.x prior to 11.2.202.270 on Linux

Vulnerability Insight
Multiple flaws due to - Dereference already freed memory - Use-after-free errors - Integer overflow and some unspecified error.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities -02 Feb13 (Linux)
OID:1.3.6.1.4.1.25623.1.0.803409
Version used: $Revision: 2923 $

References
CVE: CVE-2013-0637, CVE-2013-0638, CVE-2013-0639, CVE-2013-0642, CVE-2013-0644,
↪CVE-2013-0645, CVE-2013-0647, CVE-2013-0649, CVE-2013-1365, CVE-2013-1366, CVE
↪-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, CVE-20
↪13-1373, CVE-2013-1374
BID:57929, 57926, 57925, 57923, 57933, 57916, 57927, 57930, 57920, 57924, 57922,
↪ 57918, 57919, 57912, 57917
Other:

... continues on next page ...

... continued from previous page ...

URL:https://lwn.net/Articles/537746
URL:http://secunia.com/advisories/52166
URL:http://www.adobe.com/support/security/bulletins/apsb13-05.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities -02 Feb13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause buffer overflow, remote code execution and corrupt system memory. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to version 11.2.202.270 or later, For updates refer to http://www.adobe.com/products/flash.html

Affected Software/OS
Adobe Flash Player prior to 10.3.183.61 and 11.x prior to 11.2.202.270 on Linux

Vulnerability Insight
Multiple flaws due to - Dereference already freed memory - Use-after-free errors - Integer overflow and some unspecified error.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities -02 Feb13 (Linux)
OID:1.3.6.1.4.1.25623.1.0.803409
Version used: $Revision: 2923 $

References
CVE: CVE-2013-0637, CVE-2013-0638, CVE-2013-0639, CVE-2013-0642, CVE-2013-0644,
↪CVE-2013-0645, CVE-2013-0647, CVE-2013-0649, CVE-2013-1365, CVE-2013-1366, CVE
↪-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, CVE-20
↪13-1373, CVE-2013-1374
BID:57929, 57926, 57925, 57923, 57933, 57916, 57927, 57930, 57920, 57924, 57922,
↪ 57918, 57919, 57912, 57917
Other:
URL:https://lwn.net/Articles/537746
URL:http://secunia.com/advisories/52166
URL:http://www.adobe.com/support/security/bulletins/apsb13-05.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities August-2011 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely result in denial-of-service conditions. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 10.3.183.5 For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Flash Player versions prior to 10.3.183.5

Vulnerability Insight
Multiple flaws are caused by memory corruptions, cross-site information disclosure, buffer overflow and integer overflow errors.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities August-2011 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.902710
Version used: `$Revision: 3114 $`

References
```
CVE: CVE-2011-2130, CVE-2011-2134, CVE-2011-2137, CVE-2011-2135, CVE-2011-2136,
↪CVE-2011-2138, CVE-2011-2139, CVE-2011-2140, CVE-2011-2414, CVE-2011-2415, CVE
↪-2011-2416, CVE-2011-2417, CVE-2011-2425, CVE-2011-2424
BID:49073, 49074, 49075, 49082, 49079, 49080, 49086, 49083, 49076, 49077, 49081,
↪ 49084, 49085
Other:
  URL:http://www.adobe.com/support/security/bulletins/apsb11-21.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities August-2011 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

. . . continues on next page . . .

... continued from previous page ...

Impact
Successful exploitation will let attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely result in denial-of-service conditions. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 10.3.183.5 For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Flash Player versions prior to 10.3.183.5

Vulnerability Insight
Multiple flaws are caused by memory corruptions, cross-site information disclosure, buffer overflow and integer overflow errors.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities August-2011 (Linux)
OID:1.3.6.1.4.1.25623.1.0.902710
Version used: $Revision: 3114 $

References
CVE: CVE-2011-2130, CVE-2011-2134, CVE-2011-2137, CVE-2011-2135, CVE-2011-2136,
↪CVE-2011-2138, CVE-2011-2139, CVE-2011-2140, CVE-2011-2414, CVE-2011-2415, CVE
↪-2011-2416, CVE-2011-2417, CVE-2011-2425, CVE-2011-2424
BID:49073, 49074, 49075, 49082, 49079, 49080, 49086, 49083, 49076, 49077, 49081,
↪ 49084, 49085
Other:
URL:http://www.adobe.com/support/security/bulletins/apsb11-21.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities Dec15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 11.2.202.554

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow attackers to bypass security restrictions and execute arbitrary code on the affected system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.554 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.554 on Linux.

Vulnerability Insight
Multiple flaws exist due to, - Multiple heap buffer overflow vulnerabilities. - Multiple memory corruption vulnerabilities. - Multiple security bypass vulnerabilities. - A stack overflow vulnerability. - A type confusion vulnerability. - An integer overflow vulnerability. - A buffer overflow vulnerability. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities Dec15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806780
Version used: `$Revision: 3175 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-8045, CVE-2015-8047, CVE-2015-8048, CVE-2015-8049, CVE-2015-8050,
↪CVE-2015-8418, CVE-2015-8454, CVE-2015-8455, CVE-2015-8055, CVE-2015-8056, CVE
↪-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8060, CVE-2015-8061, CVE-20
↪15-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-
↪8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-840
↪1, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406,
↪CVE-2015-8407, CVE-2015-8408, CVE-2015-8409, CVE-2015-8410, CVE-2015-8411, CVE
↪-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8415, CVE-2015-8416, CVE-20
↪15-8417, CVE-2015-8419, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-
↪8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-842
↪8, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433,
↪CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8438, CVE
↪-2015-8439, CVE-2015-8440, CVE-2015-8441, CVE-2015-8442, CVE-2015-8443, CVE-20
↪15-8444, CVE-2015-8445, CVE-2015-8446, CVE-2015-8447, CVE-2015-8448, CVE-2015-
```

... continues on next page ...

... continued from previous page ...

```
↪8449, CVE-2015-8450, CVE-2015-8451, CVE-2015-8452, CVE-2015-8453, CVE-2015-845
↪6, CVE-2015-8457, CVE-2015-8652, CVE-2015-8653, CVE-2015-8654, CVE-2015-8655,
↪CVE-2015-8656, CVE-2015-8657, CVE-2015-8822, CVE-2015-8658, CVE-2015-8820, CVE
↪-2015-8821, CVE-2015-8823
BID:78717, 78718, 78715, 78714, 78716, 78712, 78710, 78715, 78713
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-32.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities Dec15 (Linux)

Product detection result

```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 9.0.31.0
Fixed version: 11.2.202.554
```

Impact

Successful exploitation will allow attackers to bypass security restrictions and execute arbitrary code on the affected system.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.554 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player version before 11.2.202.554 on Linux.

Vulnerability Insight

Multiple flaws exist due to, - Multiple heap buffer overflow vulnerabilities. - Multiple memory corruption vulnerabilities. - Multiple security bypass vulnerabilities. - A stack overflow vulnerability. - A type confusion vulnerability. - An integer overflow vulnerability. - A buffer overflow vulnerability. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities Dec15 (Linux)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.806780
Version used: $Revision: 3175 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-8045, CVE-2015-8047, CVE-2015-8048, CVE-2015-8049, CVE-2015-8050,
↪CVE-2015-8418, CVE-2015-8454, CVE-2015-8455, CVE-2015-8055, CVE-2015-8056, CVE
↪-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8060, CVE-2015-8061, CVE-20
↪15-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-
↪8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-840
↪1, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406,
↪CVE-2015-8407, CVE-2015-8408, CVE-2015-8409, CVE-2015-8410, CVE-2015-8411, CVE
↪-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8415, CVE-2015-8416, CVE-20
↪15-8417, CVE-2015-8419, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-
↪8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-842
↪8, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433,
↪CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8438, CVE
↪-2015-8439, CVE-2015-8440, CVE-2015-8441, CVE-2015-8442, CVE-2015-8443, CVE-20
↪15-8444, CVE-2015-8445, CVE-2015-8446, CVE-2015-8447, CVE-2015-8448, CVE-2015-
↪8449, CVE-2015-8450, CVE-2015-8451, CVE-2015-8452, CVE-2015-8453, CVE-2015-845
↪6, CVE-2015-8457, CVE-2015-8652, CVE-2015-8653, CVE-2015-8654, CVE-2015-8655,
↪CVE-2015-8656, CVE-2015-8657, CVE-2015-8822, CVE-2015-8658, CVE-2015-8820, CVE
↪-2015-8821, CVE-2015-8823
BID:78717, 78718, 78715, 78714, 78716, 78712, 78710, 78715, 78713
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb15-32.html

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities February-2011 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause a denial of service.
Impact Level: Application/System

Solution

... continues on next page ...

... continued from previous page ...

Upgrade to Adobe Flash Player version 10.2.152.26 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player versions prior to 10.2.152.26 on Linux

Vulnerability Insight
The flaws are caused by input validation errors, memory corruptions, and integer overflow errors when processing malformed Flash content, which could be exploited by attackers to execute arbitrary code by tricking a user into visiting a specially crafted web page.

Vulnerability Detection Method
Details:`Adobe Flash Player Multiple Vulnerabilities February-2011 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.801848
Version used: `$Revision: 5424 $`

References
```
CVE: CVE-2011-0558, CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571,
↪CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0575, CVE-2011-0577, CVE
↪-2011-0578, CVE-2011-0607, CVE-2011-0608
BID:46186, 46188, 46189, 46190, 46191, 46192, 46193, 46194, 46195, 46196, 46197,
↪ 46282, 46283
Other:
  URL:http://www.vupen.com/english/advisories/2011/0336
   URL:http://www.adobe.com/support/security/bulletins/apsb11-02.html
```

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities February-2011 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause a denial of service.
Impact Level: Application/System

Solution
Upgrade to Adobe Flash Player version 10.2.152.26 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player versions prior to 10.2.152.26 on Linux

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaws are caused by input validation errors, memory corruptions, and integer overflow errors when processing malformed Flash content, which could be exploited by attackers to execute arbitrary code by tricking a user into visiting a specially crafted web page.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities February-2011 (Linux)
OID:1.3.6.1.4.1.25623.1.0.801848
Version used: $Revision: 5424 $

References
CVE: CVE-2011-0558, CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, ↪CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0575, CVE-2011-0577, CVE ↪-2011-0578, CVE-2011-0607, CVE-2011-0608
BID:46186, 46188, 46189, 46190, 46191, 46192, 46193, 46194, 46195, 46196, 46197, ↪ 46282, 46283
Other:
URL:http://www.vupen.com/english/advisories/2011/0336
URL:http://www.adobe.com/support/security/bulletins/apsb11-02.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities June-2012 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attackers to bypass certain security restrictions, execute arbitrary code in the context of the browser or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.20 or 11.2.202.236 or later, For the updates refer, http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version before 10.3.183.20, Adobe Flash Player version 11.x through 11.2.202.235 on Linux.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple errors are caused, - When parsing ActionScript. - Within NPSWF32.dll when parsing certain tags. - In the 'SoundMixer.computeSpectrum()' method, which can be exploited to bypass the same-origin policy. - In the installer allows planting a binary file.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities June-2012 (Linux)
OID:1.3.6.1.4.1.25623.1.0.802873
Version used: $Revision: 5988 $

References
CVE: CVE-2012-2034, CVE-2012-2035, CVE-2012-2036, CVE-2012-2037, CVE-2012-2039,
↪CVE-2012-2038, CVE-2012-2040
BID:53887
Other:
URL:http://secunia.com/advisories/49388
URL:http://securitytracker.com/id/1027139
URL:http://www.adobe.com/support/security/bulletins/apsb12-14.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities June-2012 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attackers to bypass certain security restrictions, execute arbitrary code in the context of the browser or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 10.3.183.20 or 11.2.202.236 or later, For the updates refer, http://get.adobe.com/flashplayer/

Affected Software/OS
Adobe Flash Player version before 10.3.183.20, Adobe Flash Player version 11.x through 11.2.202.235 on Linux.

Vulnerability Insight
Multiple errors are caused, - When parsing ActionScript. - Within NPSWF32.dll when parsing certain tags. - In the 'SoundMixer.computeSpectrum()' method, which can be exploited to bypass the same-origin policy. - In the installer allows planting a binary file.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities June-2012 (Linux)
OID:1.3.6.1.4.1.25623.1.0.802873
Version used: $Revision: 5988 $

References
CVE: CVE-2012-2034, CVE-2012-2035, CVE-2012-2036, CVE-2012-2037, CVE-2012-2039,
↪CVE-2012-2038, CVE-2012-2040
BID:53887
Other:
URL:http://secunia.com/advisories/49388
URL:http://securitytracker.com/id/1027139
URL:http://www.adobe.com/support/security/bulletins/apsb12-14.html

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities May-2011 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause a denial of service condition. Impact Level: Application/System

Solution
Upgrade to Adobe Flash Player version 10.3.181.14 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version 10.2.159.1 and prior on Linux

Vulnerability Insight
The flaws are caused by memory corruptions, integer overflow errors and bounds checking errors when processing malformed Flash content, which could be exploited by attackers to execute arbitrary code by tricking a user into visiting a specially crafted web page.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities May-2011 (Linux)
OID:1.3.6.1.4.1.25623.1.0.801791
Version used: $Revision: 5424 $

References
CVE: CVE-2011-0579, CVE-2011-0618, CVE-2011-0619, CVE-2011-0620, CVE-2011-0621,

... continues on next page ...

... continued from previous page ...

↪CVE-2011-0622, CVE-2011-0623, CVE-2011-0624, CVE-2011-0625, CVE-2011-0626, CVE
↪-2011-0627
BID:47847, 47815, 47806, 47807, 47808, 47809, 47811, 47812, 47813, 47814, 47810
Other:
URL:http://www.adobe.com/support/security/bulletins/apsb11-12.html

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities May-2011 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause a denial of service condition. Impact Level: Application/System

Solution
Upgrade to Adobe Flash Player version 10.3.181.14 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version 10.2.159.1 and prior on Linux

Vulnerability Insight
The flaws are caused by memory corruptions, integer overflow errors and bounds checking errors when processing malformed Flash content, which could be exploited by attackers to execute arbitrary code by tricking a user into visiting a specially crafted web page.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities May-2011 (Linux)
OID:1.3.6.1.4.1.25623.1.0.801791
Version used: $Revision: 5424 $

References
CVE: CVE-2011-0579, CVE-2011-0618, CVE-2011-0619, CVE-2011-0620, CVE-2011-0621,
↪CVE-2011-0622, CVE-2011-0623, CVE-2011-0624, CVE-2011-0625, CVE-2011-0626, CVE
↪-2011-0627
BID:47847, 47815, 47806, 47807, 47808, 47809, 47811, 47812, 47813, 47814, 47810
Other:
URL:http://www.adobe.com/support/security/bulletins/apsb11-12.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities Sep15 (Linux)

Product detection result
`cpe:/a:adobe:flash_player:9.0.31.0`
`Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2`
`↪5623.1.0.800032)`

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 7.0.63.0`
`Fixed version: 11.2.202.521`

Impact
Successful exploitation will allow remote attackers to gain access to potentially sensitive information, conduct denial of service attack and potentially execute arbitrary code in the context of the affected user.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.521 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.521 on Linux.

Vulnerability Insight
Multiple flaws exist due to, - Multiple memory corruption errors. - Multiple unspecified errors. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities Sep15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805742
Version used: `$Revision: 2582 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2015-5567, CVE-2015-5568, CVE-2015-5570, CVE-2015-5571, CVE-2015-5572,`
. . . continues on next page . . .

... continued from previous page ...

```
↪CVE-2015-5573, CVE-2015-5574, CVE-2015-5575, CVE-2015-5576, CVE-2015-5577, CVE
↪-2015-5578, CVE-2015-5579, CVE-2015-5580, CVE-2015-5581, CVE-2015-5582, CVE-20
↪15-5584, CVE-2015-5587, CVE-2015-5588, CVE-2015-6676, CVE-2015-6677, CVE-2015-
↪6678, CVE-2015-6679, CVE-2015-6682
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-23.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities Sep15 (Linux)

Product detection result

```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 9.0.31.0
Fixed version:     11.2.202.521
```

Impact

Successful exploitation will allow remote attackers to gain access to potentially sensitive information, conduct denial of service attack and potentially execute arbitrary code in the context of the affected user.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.521 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player before version 11.2.202.521 on Linux.

Vulnerability Insight

Multiple flaws exist due to, - Multiple memory corruption errors. - Multiple unspecified errors. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities Sep15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805742
Version used: `$Revision: 2582 $`

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-5567, CVE-2015-5568, CVE-2015-5570, CVE-2015-5571, CVE-2015-5572, ↪CVE-2015-5573, CVE-2015-5574, CVE-2015-5575, CVE-2015-5576, CVE-2015-5577, CVE ↪-2015-5578, CVE-2015-5579, CVE-2015-5580, CVE-2015-5581, CVE-2015-5582, CVE-20 ↪15-5584, CVE-2015-5587, CVE-2015-5588, CVE-2015-6676, CVE-2015-6677, CVE-2015- ↪6678, CVE-2015-6679, CVE-2015-6682
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb15-23.html

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities September-2011 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause a denial of service.
Impact Level: iSystem/Application

Solution
Upgrade to Adobe Flash Player version 10.3.183.10 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player versions prior to 10.3.183.10 on Linux.

Vulnerability Insight
The flaws are due to - Stack-based buffer overflow in the ActionScript Virtual Machine (AVM) component, allows remote attackers to execute arbitrary code via unspecified vectors. - security control bypass, allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors - logic error vulnerability, allows remote attackers to cause a denial of service (browser crash) via unspecified vectors or execute arbitrary via crafted streaming media. - Cross-site scripting (XSS) vulnerability, allows remote attackers to inject arbitrary web script or HTML via a crafted URL.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities September-2011 (Linux)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.902739
Version used: $Revision: 3114 $

References
CVE: CVE-2011-2426, CVE-2011-2427, CVE-2011-2428, CVE-2011-2429, CVE-2011-2430, ↪CVE-2011-2444
BID:49714, 49715, 49716, 49718, 49717, 49710
Other:
URL:http://www.adobe.com/support/security/bulletins/apsb11-26.html

High (CVSS: 9.3)
NVT: Adobe Flash Player Multiple Vulnerabilities September-2011 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause a denial of service.
Impact Level: iSystem/Application

Solution
Upgrade to Adobe Flash Player version 10.3.183.10 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player versions prior to 10.3.183.10 on Linux.

Vulnerability Insight
The flaws are due to - Stack-based buffer overflow in the ActionScript Virtual Machine (AVM) component, allows remote attackers to execute arbitrary code via unspecified vectors. - security control bypass, allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors - logic error vulnerability, allows remote attackers to cause a denial of service (browser crash) via unspecified vectors or execute arbitrary via crafted streaming media. - Cross-site scripting (XSS) vulnerability, allows remote attackers to inject arbitrary web script or HTML via a crafted URL.

Vulnerability Detection Method
Details:Adobe Flash Player Multiple Vulnerabilities September-2011 (Linux)
OID:1.3.6.1.4.1.25623.1.0.902739
Version used: $Revision: 3114 $

References
CVE: CVE-2011-2426, CVE-2011-2427, CVE-2011-2428, CVE-2011-2429, CVE-2011-2430,

... continues on next page ...

... continued from previous page ...

↪CVE-2011-2444
BID:49714, 49715, 49716, 49718, 49717, 49710
Other:
URL:http://www.adobe.com/support/security/bulletins/apsb11-26.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities(APSB14-22)-(Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary code and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.411 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before 11.2.202.411 on Linux

Vulnerability Insight
Multiple Flaws are due to, - Two unspecified errors can be exploited to corrupt memory and subsequently execute arbitrary code. - An integer overflow error can be exploited to execute arbitrary code.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities(APSB14-22)-(Linux)
OID:1.3.6.1.4.1.25623.1.0.805004
Version used: $Revision: 3008 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0

... continues on next page ...

... continued from previous page ...

Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0558, CVE-2014-0564, CVE-2014-0569, CVE-2014-8439
BID:70437, 70442, 70441, 71289
Other:
URL:http://secunia.com/advisories/59729
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-22.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities(APSB14-22)-(Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary code and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.411 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before 11.2.202.411 on Linux

Vulnerability Insight
Multiple Flaws are due to, - Two unspecified errors can be exploited to corrupt memory and subsequently execute arbitrary code. - An integer overflow error can be exploited to execute arbitrary code.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

... continues on next page ...

... continued from previous page ...

Details:Adobe Flash Player Multiple Vulnerabilities(APSB14-22)-(Linux)
OID:1.3.6.1.4.1.25623.1.0.805004
Version used: $Revision: 3008 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0558, CVE-2014-0564, CVE-2014-0569, CVE-2014-8439
BID:70437, 70442, 70441, 71289
Other:
URL:http://secunia.com/advisories/59729
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-22.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities(APSB14-24)-(Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, bypass certain security restrictions, and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.418 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.418 on Linux

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple Flaws are due to, - An use-after-free error. - A double free error. - Multiple type confusion errors. - An error related to a permission issue. - Multiple unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities(APSB14-24)-(Linux)`
OID:1.3.6.1.4.1.25623.1.0.804795
Version used: `$Revision: 3517 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2014-0573, CVE-2014-0574, CVE-2014-0576, CVE-2014-0577, CVE-2014-0581,
↪CVE-2014-0582, CVE-2014-0583, CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, CVE
↪-2014-0588, CVE-2014-0589, CVE-2014-0590, CVE-2014-8437, CVE-2014-8438, CVE-20
↪14-8440, CVE-2014-8441, CVE-2014-8442
BID:71033, 71041, 71037, 71038, 71042, 71039, 71035, 71043, 71044, 71045, 71048,
↪ 71051, 71046, 71036, 71049, 71047, 71050, 71040
Other:
  URL:http://secunia.com/advisories/59978
   URL:http://helpx.adobe.com/security/products/flash-player/apsb14-24.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities(APSB14-24)-(Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, bypass certain security restrictions, and compromise a user's system.
Impact Level: System/Application

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.418 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.418 on Linux

Vulnerability Insight
Multiple Flaws are due to, - An use-after-free error. - A double free error. - Multiple type confusion errors. - An error related to a permission issue. - Multiple unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities(APSB14-24)-(Linux)`
OID:1.3.6.1.4.1.25623.1.0.804795
Version used: `$Revision: 3517 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2014-0573, CVE-2014-0574, CVE-2014-0576, CVE-2014-0577, CVE-2014-0581,
↪CVE-2014-0582, CVE-2014-0583, CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, CVE
↪-2014-0588, CVE-2014-0589, CVE-2014-0590, CVE-2014-8437, CVE-2014-8438, CVE-20
↪14-8440, CVE-2014-8441, CVE-2014-8442
BID:71033, 71041, 71037, 71038, 71042, 71039, 71035, 71043, 71044, 71045, 71048,
↪ 71051, 71046, 71036, 71049, 71047, 71050, 71040
Other:
  URL:http://secunia.com/advisories/59978
   URL:http://helpx.adobe.com/security/products/flash-player/apsb14-24.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities(APSB14-27)- 01 Dec14 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, bypass certain security restrictions, and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.425 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.425 on Linux

Vulnerability Insight
Multiple Flaws are due to, - An out-of-bounds read error when handling Regular Expression Objects. - Some unspecified errors. - A use-after-free error. - An error when the 'parseFloat' function is called on a specific datatype.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities(APSB14-27)- 01 Dec14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805214
Version used: `$Revision: 3517 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2014-0580, CVE-2014-0587, CVE-2014-8443, CVE-2014-9162, CVE-2014-9164,
↪CVE-2014-9163
BID:71584, 71586, 71585, 71581, 71583, 71582
Other:
  URL:http://secunia.com/advisories/61094
   URL:http://helpx.adobe.com/security/products/flash-player/apsb14-27.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities(APSB14-27)- 01 Dec14 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information, bypass certain security restrictions, and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.425 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.425 on Linux

Vulnerability Insight
Multiple Flaws are due to, - An out-of-bounds read error when handling Regular Expression Objects. - Some unspecified errors. - A use-after-free error. - An error when the 'parseFloat' function is called on a specific datatype.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities(APSB14-27)- 01 Dec14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805214
Version used: `$Revision: 3517 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2014-0580, CVE-2014-0587, CVE-2014-8443, CVE-2014-9162, CVE-2014-9164,
↪CVE-2014-9163
BID:71584, 71586, 71585, 71581, 71583, 71582
Other:
  URL:http://secunia.com/advisories/61094
   URL:http://helpx.adobe.com/security/products/flash-player/apsb14-27.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Aug14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to bypass certain security restrictions and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.400 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version 11.2.202.400 on Linux

Vulnerability Insight
Multiple Flaws are due to an unspecified error and an use-after-free error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities-01 Aug14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804744
Version used: $Revision: 3521 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0538, CVE-2014-0540, CVE-2014-0541, CVE-2014-0542, CVE-2014-0543,
↪CVE-2014-0544, CVE-2014-0545, CVE-2014-5333
BID:69192, 69190, 69191, 69194, 69195, 69196, 69197, 69320
Other:

. . . continues on next page . . .

... continued from previous page ...

URL:http://secunia.com/advisories/58593
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-18.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Aug14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to bypass certain security restrictions and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.400 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version 11.2.202.400 on Linux

Vulnerability Insight
Multiple Flaws are due to an unspecified error and an use-after-free error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities-01 Aug14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804744
Version used: $Revision: 3521 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

... continues on next page ...

... continued from previous page ...

References

```
CVE: CVE-2014-0538, CVE-2014-0540, CVE-2014-0541, CVE-2014-0542, CVE-2014-0543,
↪CVE-2014-0544, CVE-2014-0545, CVE-2014-5333
BID:69192, 69190, 69191, 69194, 69195, 69196, 69197, 69320
Other:
  URL:http://secunia.com/advisories/58593
   URL:http://helpx.adobe.com/security/products/flash-player/apsb14-18.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Dec13 (Linux)

Product detection result

```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to execute arbitrary code, cause memory corruption(denial of service) and compromise a user's system.
Impact Level: System/Application

Solution

Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.332 or later For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player before version 11.2.202.332 on Linux.

Vulnerability Insight

Flaws are due to multiple unspecified errors.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities-01 Dec13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804169
Version used: `$Revision: 3556 $`

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2013-5331, CVE-2013-5332
BID:64199, 64201
Other:
URL:http://secunia.com/advisories/55948
URL:http://helpx.adobe.com/security/products/flash-player/apsb13-28.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Dec13 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary code, cause memory corruption(denial of service) and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.332 or later For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.332 on Linux.

Vulnerability Insight
Flaws are due to multiple unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities-01 Dec13 (Linux)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.804169
Version used: $Revision: 3556 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2013-5331, CVE-2013-5332
BID:64199, 64201
Other:
URL:http://secunia.com/advisories/55948
URL:http://helpx.adobe.com/security/products/flash-player/apsb13-28.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Feb15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 11.2.202.442

Impact
Successful exploitation will allow remote attackers to corrupt memory, dereference already freed memory, execute arbitrary code or have other unspecified impacts.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.442 or later. For updates refer http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.442 on Linux.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws exists due to, - Multiple unspecified use-after-free errors. - Multiple unspecified errors due to improper validation of user-supplied input. - Multiple unspecified type confusion errors. - Multiple errors leading to overflow condition. - Multiple unspecified NULL pointer dereference errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities-01 Feb15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805270
Version used: `$Revision: 3496 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-0313, CVE-2015-0314, CVE-2015-0315, CVE-2015-0316, CVE-2015-0317,
↪CVE-2015-0318, CVE-2015-0319, CVE-2015-0320, CVE-2015-0321, CVE-2015-0322, CVE
↪-2015-0323, CVE-2015-0324, CVE-2015-0325, CVE-2015-0326, CVE-2015-0327, CVE-20
↪15-0328, CVE-2015-0329, CVE-2015-0330, CVE-2015-0331
BID:72429, 72514
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-04.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Feb15 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 9.0.31.0
Fixed version:     11.2.202.442
```

Impact
Successful exploitation will allow remote attackers to corrupt memory, dereference already freed memory, execute arbitrary code or have other unspecified impacts.
Impact Level: System/Application.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.442 or later. For updates refer http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.442 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - Multiple unspecified use-after-free errors. - Multiple unspecified errors due to improper validation of user-supplied input. - Multiple unspecified type confusion errors. - Multiple errors leading to overflow condition. - Multiple unspecified NULL pointer dereference errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities-01 Feb15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805270
Version used: `$Revision: 3496 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-0313, CVE-2015-0314, CVE-2015-0315, CVE-2015-0316, CVE-2015-0317,
↪CVE-2015-0318, CVE-2015-0319, CVE-2015-0320, CVE-2015-0321, CVE-2015-0322, CVE
↪-2015-0323, CVE-2015-0324, CVE-2015-0325, CVE-2015-0326, CVE-2015-0327, CVE-20
↪15-0328, CVE-2015-0329, CVE-2015-0330, CVE-2015-0331
BID:72429, 72514
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-04.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Jan15 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to disclose potentially sensitive information and compromise a user's system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.429 or later. For updates refer http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.429 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - An unspecified error related to improper file validation. - Another unspecified error which can be exploited to capture keystrokes. - Two unspecified errors which can be exploited to corrupt memory. - Two unspecified errors which can be exploited to cause a heap-based buffer overflow. - A type confusion error which can be exploited to corrupt memory. - An out-of-bounds read error. - An unspecified use-after-free error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities-01 Jan15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805244
Version used: `$Revision: 3496 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-0301, CVE-2015-0302, CVE-2015-0303, CVE-2015-0304, CVE-2015-0305,
↪CVE-2015-0306, CVE-2015-0307, CVE-2015-0308, CVE-2015-0309
BID:72034, 72035, 72031, 72032, 72033, 72036, 72037, 72039, 72038
Other:
  URL:http://secunia.com/advisories/62177
   URL:http://helpx.adobe.com/security/products/flash-player/apsb15-01.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Jan15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to disclose potentially sensitive information and compromise a user's system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.429 or later. For updates refer http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.429 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - An unspecified error related to improper file validation. - Another unspecified error which can be exploited to capture keystrokes. - Two unspecified errors which can be exploited to corrupt memory. - Two unspecified errors which can be exploited to cause a heap-based buffer overflow. - A type confusion error which can be exploited to corrupt memory. - An out-of-bounds read error. - An unspecified use-after-free error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities-01 Jan15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805244
Version used: $Revision: 3496 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
. . . continues on next page . . .

... continued from previous page ...

CVE: CVE-2015-0301, CVE-2015-0302, CVE-2015-0303, CVE-2015-0304, CVE-2015-0305,
↪CVE-2015-0306, CVE-2015-0307, CVE-2015-0308, CVE-2015-0309
BID:72034, 72035, 72031, 72032, 72033, 72036, 72037, 72039, 72038
Other:
URL:http://secunia.com/advisories/62177
URL:http://helpx.adobe.com/security/products/flash-player/apsb15-01.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 July13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code on the target system will cause heap-based buffer overflow or cause memory corruption via unspecified vectors.

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.297 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before 11.2.202.297 on Linux

Vulnerability Insight
Multiple unspecified error exists and an integer overflow error exists when resampling a PCM buffer.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities-01 July13 (Linux)
OID:1.3.6.1.4.1.25623.1.0.803833
Version used: $Revision: 3556 $

References
CVE: CVE-2013-3347, CVE-2013-3345, CVE-2013-3344
BID:61048, 61045, 61043
Other:
URL:http://secunia.com/advisories/53975
URL:http://www.adobe.com/support/security/bulletins/apsb13-17.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 July13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code on the target system will cause heap-based buffer overflow or cause memory corruption via unspecified vectors.

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.297 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before 11.2.202.297 on Linux

Vulnerability Insight
Multiple unspecified error exists and an integer overflow error exists when resampling a PCM buffer.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities-01 July13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803833
Version used: `$Revision: 3556 $`

References
```
CVE: CVE-2013-3347, CVE-2013-3345, CVE-2013-3344
BID:61048, 61045, 61043
Other:
  URL:http://secunia.com/advisories/53975
   URL:http://www.adobe.com/support/security/bulletins/apsb13-17.html
```

High (CVSS: 7.5)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 July14 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to bypass certain security restrictions.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.394 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.394 on Linux.

Vulnerability Insight
Multiple Flaws are due to, - An error when handling JSONP callbacks. - Multiple Unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities-01 July14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804716
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2014-4671, CVE-2014-0539, CVE-2014-0537`
`BID:68457, 68454, 68455`
`Other:`
`URL:http://secunia.com/advisories/59774`
`URL:http://helpx.adobe.com/security/products/flash-player/apsb14-17.html`

High (CVSS: 7.5)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 July14 (Linux)

Product detection result
`cpe:/a:adobe:flash_player:9.0.31.0`

... continues on next page ...

... continued from previous page ...

Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to bypass certain security restrictions.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.394 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.394 on Linux.

Vulnerability Insight
Multiple Flaws are due to, - An error when handling JSONP callbacks. - Multiple Unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities-01 July14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804716
Version used: $Revision: 3521 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-4671, CVE-2014-0539, CVE-2014-0537
BID:68457, 68454, 68455
Other:
URL:http://secunia.com/advisories/59774
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-17.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 June14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to conduct cross-site scripting attacks, bypass certain security restrictions, and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.378 or later For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.378 on Linux.

Vulnerability Insight
Multiple Flaws exists due to, - Certain unspecified input is not properly sanitised before being returned to the user. - An unspecified error can be exploited to bypass certain security restrictions. - Another unspecified error can be exploited to corrupt memory. - Another unspecified error can be exploited to bypass certain security restrictions.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities-01 June14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804647
Version used: $Revision: 3521 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0531, CVE-2014-0532, CVE-2014-0533, CVE-2014-0534, CVE-2014-0535,

. . . continues on next page . . .

... continued from previous page ...

↪CVE-2014-0536
BID:67962, 67973, 67974, 67963, 67970, 67961
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb14-16.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 June14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to conduct cross-site scripting attacks, bypass certain security restrictions, and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.378 or later For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.378 on Linux.

Vulnerability Insight
Multiple Flaws exists due to, - Certain unspecified input is not properly sanitised before being returned to the user. - An unspecified error can be exploited to bypass certain security restrictions. - Another unspecified error can be exploited to corrupt memory. - Another unspecified error can be exploited to bypass certain security restrictions.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities-01 June14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804647
Version used: $Revision: 3521 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References

CVE: CVE-2014-0531, CVE-2014-0532, CVE-2014-0533, CVE-2014-0534, CVE-2014-0535, ↪CVE-2014-0536
BID:67962, 67973, 67974, 67963, 67970, 67961
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb14-16.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 June15 (Linux)

Product detection result

cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2 ↪5623.1.0.800032)

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 7.0.63.0
Fixed version: 11.2.202.466

Impact

Successful exploitation will allow remote attackers to disclose potentially sensitive information, execute arbitrary code, cause a denial of service, bypass the same origin policy and bypass certain protection mechanism.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.466 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player before version 11.2.202.466 on Linux.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws exists due to, - An error which does not properly restrict discovery of memory addresseses. - Multiple use-after-free errors. - A memory corruption error. - An integer overflow error. - Multiple unspecified errors bypassing same origin policy. - An error due to permission issue in the flash broker for internet explorer. - A stack overflow error. - An unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities-01 June15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805586
Version used: `$Revision: 2582 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-3108, CVE-2015-3107, CVE-2015-3106, CVE-2015-3105, CVE-2015-3104,
↪CVE-2015-3103, CVE-2015-3102, CVE-2015-3101, CVE-2015-3100, CVE-2015-3099, CVE
↪-2015-3098, CVE-2015-3096
BID:75084, 75087, 75086, 75081, 75080, 75089, 75085, 75088
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-11.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 June15 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 9.0.31.0
Fixed version:     11.2.202.466
```

Impact
Successful exploitation will allow remote attackers to disclose potentially sensitive information, execute arbitrary code, cause a denial of service, bypass the same origin policy and bypass certain protection mechanism.
Impact Level: System/Application.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.466 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before version 11.2.202.466 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - An error which does not properly restrict discovery of memory addresseses. - Multiple use-after-free errors. - A memory corruption error. - An integer overflow error. - Multiple unspecified errors bypassing same origin policy. - An error due to permission issue in the flash broker for internet explorer. - A stack overflow error. - An unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities-01 June15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805586
Version used: `$Revision: 2582 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-3108, CVE-2015-3107, CVE-2015-3106, CVE-2015-3105, CVE-2015-3104,
↪CVE-2015-3103, CVE-2015-3102, CVE-2015-3101, CVE-2015-3100, CVE-2015-3099, CVE
↪-2015-3098, CVE-2015-3096
BID:75084, 75087, 75086, 75081, 75080, 75089, 75085, 75088
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb15-11.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Sep13 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary code, cause memory corruption and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.310 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before 11.2.202.310 on Linux

Vulnerability Insight
Flaws are due to multiple unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities-01 Sep13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803899
Version used: `$Revision: 3556 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2013-5324, CVE-2013-3361, CVE-2013-3362, CVE-2013-3363`
`BID:62296, 62290, 62294, 62295`
`Other:`
`URL:http://secunia.com/advisories/54697/`
`URL:https://www.adobe.com/support/security/bulletins/apsb13-21.html`

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Sep13 (Linux)

Product detection result
`cpe:/a:adobe:flash_player:9.0.31.0`
`Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2`
`↪5623.1.0.800032)`

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary code, cause memory corruption and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.310 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player before 11.2.202.310 on Linux

Vulnerability Insight
Flaws are due to multiple unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Vulnerabilities-01 Sep13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803899
Version used: `$Revision: 3556 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2013-5324, CVE-2013-3361, CVE-2013-3362, CVE-2013-3363`
`BID:62296, 62290, 62294, 62295`
`Other:`
`URL:http://secunia.com/advisories/54697/`
`URL:https://www.adobe.com/support/security/bulletins/apsb13-21.html`

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Sep14 (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.406 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.406 on Linux

Vulnerability Insight
Multiple Flaws are due to multiple unspecified errors and an use-after-free error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities-01 Sep14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804842
Version used: $Revision: 3521 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0559, CVE-2014-0557, CVE-2014-0556, CVE-2014-0555, CVE-2014-0553,
↪CVE-2014-0552, CVE-2014-0551, CVE-2014-0550, CVE-2014-0549, CVE-2014-0548, CVE
↪-2014-0547, CVE-2014-0554
BID:69704, 69701, 69696, 69706, 69707, 69703, 69702, 69700, 69699, 69705, 69695,
↪ 69697
Other:

... continues on next page ...

... continued from previous page ...

URL:http://secunia.com/advisories/60985
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-21.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Multiple Vulnerabilities-01 Sep14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to disclose potentially sensitive information and compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.406 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.406 on Linux

Vulnerability Insight
Multiple Flaws are due to multiple unspecified errors and an use-after-free error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Vulnerabilities-01 Sep14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804842
Version used: $Revision: 3521 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

... continues on next page ...

... continued from previous page ...

References

CVE: CVE-2014-0559, CVE-2014-0557, CVE-2014-0556, CVE-2014-0555, CVE-2014-0553, ↪CVE-2014-0552, CVE-2014-0551, CVE-2014-0550, CVE-2014-0549, CVE-2014-0548, CVE ↪-2014-0547, CVE-2014-0554

BID:69704, 69701, 69696, 69706, 69707, 69703, 69702, 69700, 69699, 69705, 69695, ↪ 69697

Other:

URL:http://secunia.com/advisories/60985

URL:http://helpx.adobe.com/security/products/flash-player/apsb14-21.html

High (CVSS: 9.3)

NVT: Adobe Flash Player Object Confusion Remote Code Execution Vulnerability (Linux)

Summary

This host is installed with Adobe Flash Player and is prone to object confusion remote code execution vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will let attackers to create crafted Flash content that, when loaded by the target user, will trigger an object confusion flaw and execute arbitrary code on the target system. Impact Level: System/Application

Solution

Solution type: VendorFix

Upgrade to Adobe Flash Player version 10.3.183.19 or 11.2.202.235 or later, For details refer, http://www.adobe.com/downloads/

Affected Software/OS

Adobe Flash Player version prior to 10.3.183.19 on Linux Adobe Flash Player version 11.x prior to 11.2.202.235 on Linux

Vulnerability Insight

The flaw is due to an error related to object confusion.

NOTE: Further information is not available.

Vulnerability Detection Method

Details:Adobe Flash Player Object Confusion Remote Code Execution Vulnerability (Linux)

OID:1.3.6.1.4.1.25623.1.0.802771

Version used: $Revision: 5956 $

References

CVE: CVE-2012-0779

BID:53395

... continues on next page ...

... continued from previous page ...

Other:
URL:http://secunia.com/advisories/49096/
URL:http://securitytracker.com/id/1027023
URL:http://www.adobe.com/support/security/bulletins/apsb12-09.html

High (CVSS: 9.3)
NVT: Adobe Flash Player Object Confusion Remote Code Execution Vulnerability (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to object confusion remote code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to create crafted Flash content that, when loaded by the target user, will trigger an object confusion flaw and execute arbitrary code on the target system. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 10.3.183.19 or 11.2.202.235 or later, For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version prior to 10.3.183.19 on Linux Adobe Flash Player version 11.x prior to 11.2.202.235 on Linux

Vulnerability Insight
The flaw is due to an error related to object confusion.
NOTE: Further information is not available.

Vulnerability Detection Method
Details:Adobe Flash Player Object Confusion Remote Code Execution Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.802771
Version used: $Revision: 5956 $

References
CVE: CVE-2012-0779
BID:53395
Other:
URL:http://secunia.com/advisories/49096/
URL:http://securitytracker.com/id/1027023
URL:http://www.adobe.com/support/security/bulletins/apsb12-09.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Remote Code Execution Vulnerability -June13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to remote code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code on the target system or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player 10.3.183.90 or 11.2.202.291 or later For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version 10.3.183.86 and earlier and 11.x to 11.2.202.285 on Linux

Vulnerability Insight
Unspecified flaw due to improper sanitization of user-supplied input.

Vulnerability Detection Method
Details:`Adobe Flash Player Remote Code Execution Vulnerability -June13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803662
Version used: `$Revision: 3556 $`

References
`CVE: CVE-2013-3343`
`BID:60478`
`Other:`
`URL:http://secunia.com/advisories/53751`
`URL:http://www.adobe.com/support/security/bulletins/apsb13-16.html`

High (CVSS: 10.0)
NVT: Adobe Flash Player Remote Code Execution Vulnerability -June13 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to remote code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow remote attackers to execute arbitrary code on the target system or cause a denial of service (memory corruption) via unspecified vectors. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player 10.3.183.90 or 11.2.202.291 or later For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version 10.3.183.86 and earlier and 11.x to 11.2.202.285 on Linux

Vulnerability Insight
Unspecified flaw due to improper sanitization of user-supplied input.

Vulnerability Detection Method
Details:`Adobe Flash Player Remote Code Execution Vulnerability -June13 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.803662
Version used: `$Revision: 3556 $`

References
`CVE: CVE-2013-3343`
`BID:60478`
`Other:`
`URL:http://secunia.com/advisories/53751`
`URL:http://www.adobe.com/support/security/bulletins/apsb13-16.html`

High (CVSS: 9.3)
NVT: Adobe Flash Player Remote Memory Corruption Vulnerability (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to memory corruption vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause a denial of service. Impact Level: Application/System

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 10.2.153.1 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Adobe Flash Player version 10.2.152.33 and prior on Linux.

Vulnerability Insight
The flaw is due to an error when handling the 'SWF' file, which allows attackers to execute arbitrary code or cause a denial of service via crafted flash content.

Vulnerability Detection Method
Details:`Adobe Flash Player Remote Memory Corruption Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.902401
Version used: `$Revision: 3114 $`

References
`CVE: CVE-2011-0609`
`BID:46860`
`Other:`
`URL:http://www.adobe.com/support/security/bulletins/apsb11-06.html`
`URL:http://www.adobe.com/support/security/advisories/apsa11-01.html`

High (CVSS: 9.3)
NVT: Adobe Flash Player Remote Memory Corruption Vulnerability (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to memory corruption vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code or cause a denial of service.
Impact Level: Application/System

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 10.2.153.1 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player version 10.2.152.33 and prior on Linux.

Vulnerability Insight
The flaw is due to an error when handling the 'SWF' file, which allows attackers to execute arbitrary code or cause a denial of service via crafted flash content.

Vulnerability Detection Method
Details:`Adobe Flash Player Remote Memory Corruption Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.902401

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 3114 $

References
CVE: CVE-2011-0609
BID:46860
Other:
URL:http://www.adobe.com/support/security/bulletins/apsb11-06.html
URL:http://www.adobe.com/support/security/advisories/apsa11-01.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Bypass Vulnerability Jan14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to security bypass vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to, bypass certain security restrictions and disclose certain memory informations.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.335 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.335 on Linux.

Vulnerability Insight
Flaw is due to an unspecified error and other additional weakness.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Bypass Vulnerability Jan14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804065
Version used: $Revision: 3521 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0491, CVE-2014-0492
BID:64807, 64810
Other:
URL:http://secunia.com/advisories/56267
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-02.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Bypass Vulnerability Jan14 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to security bypass vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to, bypass certain security restrictions and disclose certain memory informations.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.335 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.335 on Linux.

Vulnerability Insight
Flaw is due to an unspecified error and other additional weakness.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

... continues on next page ...

... continued from previous page ...

Details:Adobe Flash Player Security Bypass Vulnerability Jan14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804065
Version used: $Revision: 3521 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0491, CVE-2014-0492
BID:64807, 64810
Other:
URL:http://secunia.com/advisories/56267
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-02.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-10)-Linux

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 11.2.202.616

Impact
Successful exploitation of this vulnerability will allow remote attackers to bypass memory layout randomization mitigations, also leads to code execution.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.616 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.616 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The multiple flaws exists due to, - Multiple type confusion vulnerabilities. - Multiple use-after-free vulnerabilities. - Multiple memory corruption vulnerabilities. - A stack overflow vulnerability. - A vulnerability in the directory search path used to find resources.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb16-10 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.807654
Version used: `$Revision: 5557 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2016-1006, CVE-2016-1011, CVE-2016-1012, CVE-2016-1013, CVE-2016-1014,
↪CVE-2016-1015, CVE-2016-1016, CVE-2016-1017, CVE-2016-1018, CVE-2016-1019, CVE
↪-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-20
↪16-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-
↪1030, CVE-2016-1031, CVE-2016-1032, CVE-2016-1033
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-10.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-10)-Linux

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 9.0.31.0
Fixed version:     11.2.202.616
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to bypass memory layout randomization mitigations, also leads to code execution.
Impact Level: System/Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.616 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.616 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - Multiple type confusion vulnerabilities. - Multiple use-after-free vulnerabilities. - Multiple memory corruption vulnerabilities. - A stack overflow vulnerability. - A vulnerability in the directory search path used to find resources.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb16-10 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.807654
Version used: `$Revision: 5557 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2016-1006, CVE-2016-1011, CVE-2016-1012, CVE-2016-1013, CVE-2016-1014,
↪CVE-2016-1015, CVE-2016-1016, CVE-2016-1017, CVE-2016-1018, CVE-2016-1019, CVE
↪-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-20
↪16-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-
↪1030, CVE-2016-1031, CVE-2016-1032, CVE-2016-1033
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-10.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-15)-Linux

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 11.2.202.621

Impact
Successful exploitation of this vulnerability will allow remote attackers to execute arbitrary code.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.621 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.621 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - Multiple type confusion vulnerabilities. - Multiple use-after-free vulnerabilities. - A heap buffer overflow vulnerability. - A buffer overflow vulnerability. - Multiple memory corruption vulnerabilities. - A vulnerability in the directory search path used to find resources.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Updates(apsb16-15)-Linux
OID:1.3.6.1.4.1.25623.1.0.808104
Version used: $Revision: 5675 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-1096, CVE-2016-1097, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100,
↪CVE-2016-1101, CVE-2016-1102, CVE-2016-1103, CVE-2016-1104, CVE-2016-1105, CVE
↪-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-20
↪16-4108, CVE-2016-4109, CVE-2016-4110, CVE-2016-4111, CVE-2016-4112, CVE-2016-
↪4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4116, CVE-2016-4117, CVE-2016-412
↪0, CVE-2016-4121, CVE-2016-4160, CVE-2016-4161, CVE-2016-4162, CVE-2016-4163
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb16-15.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-15)-Linux

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.621

Impact
Successful exploitation of this vulnerability will allow remote attackers to execute arbitrary code.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.621 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.621 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - Multiple type confusion vulnerabilities. - Multiple use-after-free vulnerabilities. - A heap buffer overflow vulnerability. - A buffer overflow vulnerability. - Multiple memory corruption vulnerabilities. - A vulnerability in the directory search path used to find resources.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Updates(apsb16-15)-Linux
OID:1.3.6.1.4.1.25623.1.0.808104
Version used: $Revision: 5675 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-1096, CVE-2016-1097, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100,

. . . continues on next page . . .

... continued from previous page ...

```
↪CVE-2016-1101, CVE-2016-1102, CVE-2016-1103, CVE-2016-1104, CVE-2016-1105, CVE
↪-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-20
↪16-4108, CVE-2016-4109, CVE-2016-4110, CVE-2016-4111, CVE-2016-4112, CVE-2016-
↪4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4116, CVE-2016-4117, CVE-2016-412
↪0, CVE-2016-4121, CVE-2016-4160, CVE-2016-4161, CVE-2016-4162, CVE-2016-4163
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-15.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-18)-Linux

Product detection result

```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.0.63.0
Fixed version:     11.2.202.626
```

Impact

Successful exploitation will allow remote attackers to bypass the same-origin-policy and lead to information disclosure, and code execution.
Impact Level: System/Application

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.626 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player version before 11.2.202.626 on Linux.

Vulnerability Insight

The multiple flaws exists due to, - A type confusion vulnerabilities. - The use-after-free vulnerabilities. - The heap buffer overflow vulnerabilities. - The memory corruption vulnerabilities. - A vulnerability in the directory search path used to find resources.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb16-18 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.808169

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 5534 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-4122, CVE-2016-4123, CVE-2016-4124, CVE-2016-4125, CVE-2016-4127,
↪CVE-2016-4128, CVE-2016-4129, CVE-2016-4130, CVE-2016-4131, CVE-2016-4132, CVE
↪-2016-4133, CVE-2016-4134, CVE-2016-4135, CVE-2016-4136, CVE-2016-4137, CVE-20
↪16-4138, CVE-2016-4139, CVE-2016-4140, CVE-2016-4141, CVE-2016-4142, CVE-2016-
↪4143, CVE-2016-4144, CVE-2016-4145, CVE-2016-4146, CVE-2016-4147, CVE-2016-414
↪8, CVE-2016-4149, CVE-2016-4150, CVE-2016-4151, CVE-2016-4152, CVE-2016-4153,
↪CVE-2016-4154, CVE-2016-4155, CVE-2016-4156, CVE-2016-4166, CVE-2016-4171
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb16-18.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-18)-Linux

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.626

Impact
Successful exploitation will allow remote attackers to bypass the same-origin-policy and lead to information disclosure, and code execution.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.626 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Adobe Flash Player version before 11.2.202.626 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - A type confusion vulnerabilities. - The use-after-free vulnerabilities. - The heap buffer overflow vulnerabilities. - The memory corruption vulnerabilities. - A vulnerability in the directory search path used to find resources.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb16-18 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.808169
Version used: `$Revision: 5534 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2016-4122, CVE-2016-4123, CVE-2016-4124, CVE-2016-4125, CVE-2016-4127,
↪CVE-2016-4128, CVE-2016-4129, CVE-2016-4130, CVE-2016-4131, CVE-2016-4132, CVE
↪-2016-4133, CVE-2016-4134, CVE-2016-4135, CVE-2016-4136, CVE-2016-4137, CVE-20
↪16-4138, CVE-2016-4139, CVE-2016-4140, CVE-2016-4141, CVE-2016-4142, CVE-2016-
↪4143, CVE-2016-4144, CVE-2016-4145, CVE-2016-4146, CVE-2016-4147, CVE-2016-414
↪8, CVE-2016-4149, CVE-2016-4150, CVE-2016-4151, CVE-2016-4152, CVE-2016-4153,
↪CVE-2016-4154, CVE-2016-4155, CVE-2016-4156, CVE-2016-4166, CVE-2016-4171
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-18.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-25)-Linux

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 7.0.63.0
Fixed version:     11.2.202.632
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation of this vulnerability will allow remote attackers lead to information disclosure, and code execution.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.632 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.632 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - A race condition vulnerability. - A type confusion vulnerabilities. - An use-after-free vulnerabilities. - A heap buffer overflow vulnerability. - A memory corruption vulnerabilities. - A stack corruption vulnerabilities. - A security bypass vulnerability.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb16-25 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.808579
Version used: `$Revision: 5732 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2016-4172, CVE-2016-4173, CVE-2016-4174, CVE-2016-4175, CVE-2016-4176,
↪CVE-2016-4177, CVE-2016-4178, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE
↪-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-20
↪16-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-
↪4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4222, CVE-2016-422
↪3, CVE-2016-4224, CVE-2016-4225, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228,
↪CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, CVE-2016-4232, CVE-2016-4233, CVE
↪-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-20
↪16-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-
↪4244, CVE-2016-4245, CVE-2016-4246, CVE-2016-4247, CVE-2016-4248, CVE-2016-424
↪9, CVE-2016-7020
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-25.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-25)-Linux

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.632

Impact
Successful exploitation of this vulnerability will allow remote attackers lead to information disclosure, and code execution.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.632 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.632 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - A race condition vulnerability. - A type confusion vulnerabilities. - An use-after-free vulnerabilities. - A heap buffer overflow vulnerability. - A memory corruption vulnerabilities. - A stack corruption vulnerabilities. - A security bypass vulnerability.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Updates(apsb16-25)-Linux
OID:1.3.6.1.4.1.25623.1.0.808579
Version used: $Revision: 5732 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-4172, CVE-2016-4173, CVE-2016-4174, CVE-2016-4175, CVE-2016-4176,
↪CVE-2016-4177, CVE-2016-4178, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE
↪-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-20

... continues on next page ...

... continued from previous page ...

```
↪16-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-
↪4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4222, CVE-2016-422
↪3, CVE-2016-4224, CVE-2016-4225, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228,
↪CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, CVE-2016-4232, CVE-2016-4233, CVE
↪-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-20
↪16-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-
↪4244, CVE-2016-4245, CVE-2016-4246, CVE-2016-4247, CVE-2016-4248, CVE-2016-424
↪9, CVE-2016-7020
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-25.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-29)-Linux

Product detection result

```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.0.63.0
Fixed version:     11.2.202.635
```

Impact

Successful exploitation of this vulnerability will allow remote attackers lead to code execution and information disclosure.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.635 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player version before 11.2.202.635 on Linux.

Vulnerability Insight

The multiple flaws exists due to, - An integer overflow vulnerability. - The use-after-free vulnerabilities. - The security bypass vulnerabilities. - The memory corruption vulnerabilities.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.

... continues on next page ...

... continued from previous page ...

Details:Adobe Flash Player Security Updates(apsb16-29)-Linux
OID:1.3.6.1.4.1.25623.1.0.809222
Version used: $Revision: 5813 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-4271, CVE-2016-4272, CVE-2016-4274, CVE-2016-4275, CVE-2016-4276,
↪CVE-2016-4277, CVE-2016-4278, CVE-2016-4279, CVE-2016-4280, CVE-2016-4281, CVE
↪-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-4287, CVE-20
↪16-6921, CVE-2016-6922, CVE-2016-6923, CVE-2016-6924, CVE-2016-6925, CVE-2016-
↪6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, CVE-2016-693
↪2, CVE-2016-4182, CVE-2016-4237, CVE-2016-4238
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb16-29.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-29)-Linux

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.635

Impact
Successful exploitation of this vulnerability will allow remote attackers lead to code execution and information disclosure.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.635 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Adobe Flash Player version before 11.2.202.635 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - An integer overflow vulnerability. - The use-after-free vulnerabilities. - The security bypass vulnerabilities. - The memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb16-29 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.809222
Version used: `$Revision: 5813 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2016-4271, CVE-2016-4272, CVE-2016-4274, CVE-2016-4275, CVE-2016-4276,
↪CVE-2016-4277, CVE-2016-4278, CVE-2016-4279, CVE-2016-4280, CVE-2016-4281, CVE
↪-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-4287, CVE-20
↪16-6921, CVE-2016-6922, CVE-2016-6923, CVE-2016-6924, CVE-2016-6925, CVE-2016-
↪6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, CVE-2016-693
↪2, CVE-2016-4182, CVE-2016-4237, CVE-2016-4238
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-29.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-32)-Linux

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 7.0.63.0
Fixed version:     11.2.202.637
```

Impact
Successful exploitation of this vulnerability will allow remote attackers lead to code execution.

... continues on next page ...

... continued from previous page ...

Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.637 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.637 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - a type confusion vulnerability. - use-after-free vulnerabilities. - memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb16-32 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.809442
Version used: `$Revision: 5675 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2016-4273, CVE-2016-4286, CVE-2016-6981, CVE-2016-6982, CVE-2016-6983,
↪CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6987, CVE-2016-6989, CVE
↪-2016-6990, CVE-2016-6992
BID:93490, 93497, 93492
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-32.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-32)-Linux

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.637

Impact
Successful exploitation of this vulnerability will allow remote attackers lead to code execution.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.637 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.637 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - a type confusion vulnerability. - use-after-free vulnerabilities. - memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Updates(apsb16-32)-Linux
OID:1.3.6.1.4.1.25623.1.0.809442
Version used: $Revision: 5675 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-4273, CVE-2016-4286, CVE-2016-6981, CVE-2016-6982, CVE-2016-6983,
↪CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6987, CVE-2016-6989, CVE
↪-2016-6990, CVE-2016-6992
BID:93490, 93497, 93492
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb16-32.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-36)-Linux

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 7.0.63.0`
`Fixed version: 11.2.202.643`

Impact
Successful exploitation of this vulnerability will allow remote attackers to take control of the affected system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.643 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.643 on Linux.

Vulnerability Insight
The Flaw exists due to, a use-after-free vulnerability

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb16-36 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.809463
Version used: `$Revision: 5513 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2016-7855`
`Other:`
`URL:https://helpx.adobe.com/security/products/flash-player/apsb16-36.html`

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-36)-Linux

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.643

Impact
Successful exploitation of this vulnerability will allow remote attackers to take control of the affected system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.643 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.643 on Linux.

Vulnerability Insight
The Flaw exists due to, a use-after-free vulnerability

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Updates(apsb16-36)-Linux
OID:1.3.6.1.4.1.25623.1.0.809463
Version used: $Revision: 5513 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-7855
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb16-36.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-39)-Linux

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 24.0.0.186

Impact
Successful exploitation of this vulnerability will allow remote attackers to take control of the affected system, and lead to code execution.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 24.0.0.186 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 24.0.0.186 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - An use-after-free vulnerabilities. - The buffer overflow vulnerabilities. - The memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Updates(apsb16-39)-Linux
OID:1.3.6.1.4.1.25623.1.0.810312
Version used: $Revision: 4760 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-7867, CVE-2016-7868, CVE-2016-7869, CVE-2016-7870, CVE-2016-7871,
↪CVE-2016-7872, CVE-2016-7873, CVE-2016-7874, CVE-2016-7875, CVE-2016-7876, CVE

. . . continues on next page . . .

... continued from previous page ...

```
↪-2016-7877, CVE-2016-7878, CVE-2016-7879, CVE-2016-7880, CVE-2016-7881, CVE-20
↪16-7890, CVE-2016-7892
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-39.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-39)-Linux

Product detection result

```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 9.0.31.0
Fixed version:     24.0.0.186
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to take control of the affected system, and lead to code execution.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 24.0.0.186 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player version before 24.0.0.186 on Linux.

Vulnerability Insight

The multiple flaws exists due to, - An use-after-free vulnerabilities. - The buffer overflow vulnerabilities. - The memory corruption vulnerabilities.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb16-39 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.810312
Version used: `$Revision: 4760 $`

Product Detection Result

Product: `cpe:/a:adobe:flash_player:9.0.31.0`

... continues on next page ...

... continued from previous page ...

Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References

CVE: CVE-2016-7867, CVE-2016-7868, CVE-2016-7869, CVE-2016-7870, CVE-2016-7871, CVE-2016-7872, CVE-2016-7873, CVE-2016-7874, CVE-2016-7875, CVE-2016-7876, CVE-2016-7877, CVE-2016-7878, CVE-2016-7879, CVE-2016-7880, CVE-2016-7881, CVE-2016-7890, CVE-2016-7892
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb16-39.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb17-02)-Linux

Product detection result

cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.800032)

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 7.0.63.0
Fixed version: 24.0.0.194

Impact

Successful exploitation of this vulnerability will allow remote attackers to take control of the affected system, lead to code execution and information disclosure.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 24.0.0.194 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player version before 24.0.0.194 on Linux.

Vulnerability Insight

The multiple flaws exists due to, - A security bypass vulnerability. - An use-after-free vulnerabilities. - The heap buffer overflow vulnerabilities. - The memory corruption vulnerabilities.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Updates(apsb17-02)-Linux
OID:1.3.6.1.4.1.25623.1.0.810330
Version used: $Revision: 4983 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2017-2925, CVE-2017-2926, CVE-2017-2927, CVE-2017-2928, CVE-2017-2930,
↪CVE-2017-2931, CVE-2017-2932, CVE-2017-2933, CVE-2017-2934, CVE-2017-2935, CVE
↪-2017-2936, CVE-2017-2937, CVE-2017-2938
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb17-02.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb17-02)-Linux

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 24.0.0.194

Impact
Successful exploitation of this vulnerability will allow remote attackers to take control of the affected system, lead to code execution and information disclosure.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 24.0.0.194 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 24.0.0.194 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The multiple flaws exists due to, - A security bypass vulnerability. - An use-after-free vulnerabilities. - The heap buffer overflow vulnerabilities. - The memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Updates(apsb17-02)-Linux
OID:1.3.6.1.4.1.25623.1.0.810330
Version used: $Revision: 4983 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2017-2925, CVE-2017-2926, CVE-2017-2927, CVE-2017-2928, CVE-2017-2930,
↪CVE-2017-2931, CVE-2017-2932, CVE-2017-2933, CVE-2017-2934, CVE-2017-2935, CVE
↪-2017-2936, CVE-2017-2937, CVE-2017-2938
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb17-02.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb17-04)-Linux

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 24.0.0.221

Impact
Successful exploitation of this vulnerabilities will allow remote attackers to execute arbitrary code on the target user's system and that could potentially allow an attacker to take control of the affected system.
Impact Level: System/Application

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to Adobe Flash Player version 24.0.0.221 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 24.0.0.221 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - A type confusion vulnerability. - Multiple use-after-free vulnerabilities. - An integer overflow vulnerability. - Multiple heap buffer overflow vulnerabilities. - Multiple memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb17-04 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.810552
Version used: `$Revision: 5301 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2017-2982, CVE-2017-2984, CVE-2017-2985, CVE-2017-2986, CVE-2017-2987,
↪CVE-2017-2988, CVE-2017-2990, CVE-2017-2991, CVE-2017-2992, CVE-2017-2993, CVE
↪-2017-2994, CVE-2017-2995, CVE-2017-2996
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb17-04.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb17-04)-Linux

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 9.0.31.0
Fixed version:     24.0.0.221
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation of this vulnerabilities will allow remote attackers to execute arbitrary code on the target user's system and that could potentially allow an attacker to take control of the affected system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 24.0.0.221 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 24.0.0.221 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - A type confusion vulnerability. - Multiple use-after-free vulnerabilities. - An integer overflow vulnerability. - Multiple heap buffer overflow vulnerabilities. - Multiple memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb17-04 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.810552
Version used: `$Revision: 5301 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2017-2982, CVE-2017-2984, CVE-2017-2985, CVE-2017-2986, CVE-2017-2987,
↪CVE-2017-2988, CVE-2017-2990, CVE-2017-2991, CVE-2017-2992, CVE-2017-2993, CVE
↪-2017-2994, CVE-2017-2995, CVE-2017-2996
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb17-04.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb17-10)-Linux

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 7.0.63.0`
`Fixed version: 25.0.0.148`

Impact
Successful exploitation of this vulnerabilities will allow remote attackers to execute arbitrary code on the target user's system and that could potentially allow an attacker to take control of the affected system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 25.0.0.148, or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 25.0.0.148 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - Use-after-free vulnerabilities that could lead to code execution. - Memory corruption vulnerabilities that could lead to code execution.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates( apsb17-10 )-Linux`
OID:1.3.6.1.4.1.25623.1.0.810840
Version used: `$Revision: 5941 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2017-3058, CVE-2017-3059, CVE-2017-3060, CVE-2017-3061, CVE-2017-3062,`
`↪CVE-2017-3063, CVE-2017-3064, CVE-2015-5122, CVE-2015-5123`
`BID:97551, 97557, 75712, 75710`
`Other:`
`URL:https://helpx.adobe.com/security/products/flash-player/apsb17-10.html`

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb17-10)-Linux

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 25.0.0.148

Impact
Successful exploitation of this vulnerabilities will allow remote attackers to execute arbitrary code on the target user's system and that could potentially allow an attacker to take control of the affected system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 25.0.0.148, or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 25.0.0.148 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - Use-after-free vulnerabilities that could lead to code execution. - Memory corruption vulnerabilities that could lead to code execution.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Updates(apsb17-10)-Linux
OID:1.3.6.1.4.1.25623.1.0.810840
Version used: $Revision: 5941 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2017-3058, CVE-2017-3059, CVE-2017-3060, CVE-2017-3061, CVE-2017-3062,

... continues on next page ...

... continued from previous page ...

```
↪CVE-2017-3063, CVE-2017-3064, CVE-2015-5122, CVE-2015-5123
BID:97551, 97557, 75712, 75710
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb17-10.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-37) - Linux

Product detection result

```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 7.0.63.0
Fixed version:     11.2.202.644
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to take control of the affected system, and lead to code execution.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.644 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player version before 11.2.202.644 on Linux.

Vulnerability Insight

The multiple flaws exists due to, - A type confusion vulnerabilities. - An use-after-free vulnerabilities.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates(apsb16-37) - Linux`
OID:1.3.6.1.4.1.25623.1.0.809469
Version used: `$Revision: 5712 $`

Product Detection Result

Product: `cpe:/a:adobe:flash_player:9.0.31.0`

... continues on next page ...

... continued from previous page ...

Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References

CVE: CVE-2016-7857, CVE-2016-7858, CVE-2016-7859, CVE-2016-7860, CVE-2016-7861, ↪CVE-2016-7862, CVE-2016-7863, CVE-2016-7864, CVE-2016-7865
BID:94153
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb16-37.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb16-37) - Linux

Product detection result

cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2 ↪5623.1.0.800032)

Summary

This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 9.0.31.0
Fixed version: 11.2.202.644

Impact

Successful exploitation of this vulnerability will allow remote attackers to take control of the affected system, and lead to code execution.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.644 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player version before 11.2.202.644 on Linux.

Vulnerability Insight

The multiple flaws exists due to, - A type confusion vulnerabilities. - An use-after-free vulnerabilities.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.

... continues on next page ...

... continued from previous page ...

Details:Adobe Flash Player Security Updates(apsb16-37) - Linux
OID:1.3.6.1.4.1.25623.1.0.809469
Version used: $Revision: 5712 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-7857, CVE-2016-7858, CVE-2016-7859, CVE-2016-7860, CVE-2016-7861,
↪CVE-2016-7862, CVE-2016-7863, CVE-2016-7864, CVE-2016-7865
BID:94153
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb16-37.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb17-07)-Linux

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 25.0.0.127

Impact
Successful exploitation of this vulnerability will allow remote attackers to execute arbitrary code on the target user's system and that could potentially allow an attacker to take control of the affected system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 25.0.0.127, or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 25.0.0.127 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple flaws exists due to, - A buffer overflow vulnerability. - The memory corruption vulnerabilities. - A random number generator vulnerability used for constant blinding. - The use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates(apsb17-07)-Linux`
OID:1.3.6.1.4.1.25623.1.0.810806
Version used: `$Revision: 5582 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2017-2997, CVE-2017-2998, CVE-2017-2999, CVE-2017-3000, CVE-2017-3001,
↪CVE-2017-3002, CVE-2017-3003
BID:96860, 96866, 96862, 96861
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb17-07.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates(apsb17-07)-Linux

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 9.0.31.0
Fixed version:     25.0.0.127
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to execute arbitrary code on the target user's system and that could potentially allow an attacker to take control of the affected system.
Impact Level: System/Application.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 25.0.0.127, or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 25.0.0.127 on Linux.

Vulnerability Insight
Multiple flaws exists due to, - A buffer overflow vulnerability. - The memory corruption vulnerabilities. - A random number generator vulnerability used for constant blinding. - The use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates(apsb17-07)-Linux`
OID:1.3.6.1.4.1.25623.1.0.810806
Version used: `$Revision: 5582 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2017-2997, CVE-2017-2998, CVE-2017-2999, CVE-2017-3000, CVE-2017-3001,
↪CVE-2017-3002, CVE-2017-3003
BID:96860, 96866, 96862, 96861
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb17-07.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates-APSB16-08 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 7.0.63.0`

... continues on next page ...

... continued from previous page ...

Fixed version: 11.2.202.577

Impact
Successful exploitation of this vulnerability will allow remote attackers to execute arbitrary code.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.577 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.577 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - An integer overflow vulnerabilities. - A use-after-free vulnerabilities. - A heap overflow vulnerability. - The memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Security Updates-APSB16-08 (Linux)
OID:1.3.6.1.4.1.25623.1.0.807611
Version used: $Revision: 5568 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0963, CVE-2016-0986,
↪CVE-2016-0987, CVE-2016-0988, CVE-2016-0989, CVE-2016-0990, CVE-2016-0991, CVE
↪-2016-0992, CVE-2016-0993, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-20
↪16-0997, CVE-2016-0998, CVE-2016-0999, CVE-2016-1000, CVE-2016-1001, CVE-2016-
↪1002, CVE-2016-1005, CVE-2016-1010
Other:
URL:https://helpx.adobe.com/security/products/flash-player/apsb16-08.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Security Updates-APSB16-08 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 9.0.31.0`
`Fixed version: 11.2.202.577`

Impact
Successful exploitation of this vulnerability will allow remote attackers to execute arbitrary code.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.577 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.577 on Linux.

Vulnerability Insight
The multiple flaws exists due to, - An integer overflow vulnerabilities. - A use-after-free vulnerabilities. - A heap overflow vulnerability. - The memory corruption vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Security Updates-APSB16-08 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807611
Version used: `$Revision: 5568 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0963, CVE-2016-0986,
↪CVE-2016-0987, CVE-2016-0988, CVE-2016-0989, CVE-2016-0990, CVE-2016-0991, CVE
↪-2016-0992, CVE-2016-0993, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-20
↪16-0997, CVE-2016-0998, CVE-2016-0999, CVE-2016-1000, CVE-2016-1001, CVE-2016-
↪1002, CVE-2016-1005, CVE-2016-1010
Other:
  URL:https://helpx.adobe.com/security/products/flash-player/apsb16-08.html
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Unspecified Code Execution Vulnerability - Jan15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to unspecified arbitrary code execution vulnerability.

Vulnerability Detection Result
Installed version: 7.0.63.0
Fixed version: 11.2.202.440

Impact
Successful exploitation will allow remote attackers to compromise a user's system.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.440 or later. For updates refer http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player through version 11.2.202.438 on Linux.

Vulnerability Insight
The flaw exists due to some unspecified error and double-free flaw that is triggered as user-supplied input is not properly validated.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Unspecified Code Execution Vulnerability - Jan15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805261
Version used: $Revision: 3496 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-0311, CVE-2015-0312
BID:72283, 72343

. . . continues on next page . . .

... continued from previous page ...

```
Other:
  URL:http://secunia.com/advisories/62432
   URL:http://helpx.adobe.com/security/products/flash-player/apsa15-01.html
   URL:http://www.rapid7.com/db/vulnerabilities/adobe-flash-apsb15-03-cve-2015-0
↪312
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Unspecified Code Execution Vulnerability - Jan15 (Linux)

Product detection result

```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

Summary

This host is installed with Adobe Flash Player and is prone to unspecified arbitrary code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 9.0.31.0
Fixed version:     11.2.202.440
```

Impact

Successful exploitation will allow remote attackers to compromise a user's system.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.440 or later. For updates refer http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player through version 11.2.202.438 on Linux.

Vulnerability Insight

The flaw exists due to some unspecified error and double-free flaw that is triggered as user-supplied input is not properly validated.

Vulnerability Detection Method

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Unspecified Code Execution Vulnerability - Jan15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805261
Version used: `$Revision: 3496 $`

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References

CVE: CVE-2015-0311, CVE-2015-0312
BID:72283, 72343
Other:
URL:http://secunia.com/advisories/62432
URL:http://helpx.adobe.com/security/products/flash-player/apsa15-01.html
URL:http://www.rapid7.com/db/vulnerabilities/adobe-flash-apsb15-03-cve-2015-0
↪312

High (CVSS: 10.0)
NVT: Adobe Flash Player Unspecified Memory Corruption Vulnerability - Jan15 (Linux)

Product detection result

cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary

This host is installed with Adobe Flash Player and is prone to unspecified memory corruption vulnerability.

Vulnerability Detection Result

Installed version: 7.0.63.0
Fixed version: 11.2.202.438

Impact

Successful exploitation will allow remote attackers to bypass certain security restrictions and potentially conduct more severe attacks.
Impact Level: System/Application.

Solution

Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.438 or later. For updates refer http://get.adobe.com/flashplayer

Affected Software/OS

Adobe Flash Player before version 11.2.202.438 on Linux.

Vulnerability Insight

The flaw exists due to some unspecified error.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Unspecified Memory Corruption Vulnerability - Jan15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805258
Version used: $Revision: 3496 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-0310
BID:72261
Other:
URL:http://secunia.com/advisories/62452
URL:http://helpx.adobe.com/security/products/flash-player/apsb15-02.html

High (CVSS: 10.0)
NVT: Adobe Flash Player Unspecified Memory Corruption Vulnerability - Jan15 (Linux)

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to unspecified memory corruption vulnerability.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.438

Impact
Successful exploitation will allow remote attackers to bypass certain security restrictions and potentially conduct more severe attacks.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.438 or later. For updates refer http://get.adobe.com/flashplayer

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Adobe Flash Player before version 11.2.202.438 on Linux.

Vulnerability Insight
The flaw exists due to some unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Unspecified Memory Corruption Vulnerability - Jan15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805258
Version used: `$Revision: 3496 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
`CVE: CVE-2015-0310`
`BID:72261`
`Other:`
`URL:http://secunia.com/advisories/62452`
`URL:http://helpx.adobe.com/security/products/flash-player/apsb15-02.html`

High (CVSS: 10.0)
NVT: Adobe Flash Player Use-After-Free Vulnerability July15 (Linux)

Product detection result
`cpe:/a:adobe:flash_player:9.0.31.0`
`Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2`
`↪5623.1.0.800032)`

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 7.0.63.0`
`Fixed version: 11.2.202.481`

Impact
Successful exploitation will allow remote attackers to gain access to potentially sensitive information, conduct denial of service attack and potentially execute arbitrary code in the context of the affected user.

... continues on next page ...

... continued from previous page ...

Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.481 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player versions before 11.2.202.481 on Linux.

Vulnerability Insight
Multiple flaws exist due to, - An use-after-free error in 'ByteArray' class. - Multiple heap based buffer overflow errors. - Multiple memory corruption errors. - Multiple null pointer dereference errors. - Multiple unspecified errors. - A type confusion error. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Use-After-Free Vulnerability July15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.805904
Version used: `$Revision: 2582 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2015-5119, CVE-2014-0578, CVE-2015-3114, CVE-2015-3115, CVE-2015-3116,
↪CVE-2015-3117, CVE-2015-3118, CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, CVE
↪-2015-3122, CVE-2015-3123, CVE-2015-3124, CVE-2015-3125, CVE-2015-3126, CVE-20
↪15-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3130, CVE-2015-3131, CVE-2015-
↪3132, CVE-2015-3133, CVE-2015-3134, CVE-2015-3135, CVE-2015-3136, CVE-2015-313
↪7, CVE-2015-4428, CVE-2015-4429, CVE-2015-4430, CVE-2015-4431, CVE-2015-4432,
↪CVE-2015-4433, CVE-2015-5116, CVE-2015-5117, CVE-2015-5118
BID:75568, 75594, 75593, 75591, 75590, 75595, 75596, 75592
Other:
  URL:https://www.kb.cert.org/vuls/id/561288
   URL:https://helpx.adobe.com/security/products/flash-player/apsa15-03.html
   URL:https://helpx.adobe.com/security/products/flash-player/apsb15-16.html
   URL:http://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flas
↪h-player-flaws-more-pocs-found-in-hacking-team-leak
```

High (CVSS: 10.0)
NVT: Adobe Flash Player Use-After-Free Vulnerability July15 (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 9.0.31.0
Fixed version: 11.2.202.481

Impact
Successful exploitation will allow remote attackers to gain access to potentially sensitive information, conduct denial of service attack and potentially execute arbitrary code in the context of the affected user.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to Adobe Flash Player version 11.2.202.481 or later. For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player versions before 11.2.202.481 on Linux.

Vulnerability Insight
Multiple flaws exist due to, - An use-after-free error in 'ByteArray' class. - Multiple heap based buffer overflow errors. - Multiple memory corruption errors. - Multiple null pointer dereference errors. - Multiple unspecified errors. - A type confusion error. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Use-After-Free Vulnerability July15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805904
Version used: $Revision: 2582 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2015-5119, CVE-2014-0578, CVE-2015-3114, CVE-2015-3115, CVE-2015-3116,

... continues on next page ...

... continued from previous page ...

```
↪CVE-2015-3117, CVE-2015-3118, CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, CVE
↪-2015-3122, CVE-2015-3123, CVE-2015-3124, CVE-2015-3125, CVE-2015-3126, CVE-20
↪15-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3130, CVE-2015-3131, CVE-2015-
↪3132, CVE-2015-3133, CVE-2015-3134, CVE-2015-3135, CVE-2015-3136, CVE-2015-313
↪7, CVE-2015-4428, CVE-2015-4429, CVE-2015-4430, CVE-2015-4431, CVE-2015-4432,
↪CVE-2015-4433, CVE-2015-5116, CVE-2015-5117, CVE-2015-5118
BID:75568, 75594, 75593, 75591, 75590, 75595, 75596, 75592
Other:
  URL:https://www.kb.cert.org/vuls/id/561288
   URL:https://helpx.adobe.com/security/products/flash-player/apsa15-03.html
   URL:https://helpx.adobe.com/security/products/flash-player/apsb15-16.html
   URL:http://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flas
↪h-player-flaws-more-pocs-found-in-hacking-team-leak
```

High (CVSS: 9.3)
NVT: Adobe Flash Player/Air Multiple DoS Vulnerabilities - Aug09 (Linux)

Summary
This host is installed with Adobe Flash Player/Air and is prone to multiple Denial of Service vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code, gain elevated privileges, gain knowledge of certain information and conduct clickjacking attacks. Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Air 1.5.2 or Adobe Flash Player 9.0.246.0 or 10.0.32.18 http://get.adobe.com/air http://www.adobe.com/support/flashplayer/downloads.html

Affected Software/OS
Adobe AIR version prior to 1.5.2 Adobe Flash Player 9 version prior to 9.0.246.0 Adobe Flash Player 10 version prior to 10.0.32.18 on Linux.

Vulnerability Insight
Multiple vulnerabilities which can be to exploited to cause memory corruption, null pointer, privilege escalation, heap-based buffer overflow, local sandbox bypass, and input validation errors when processing specially crafted web pages.

Vulnerability Detection Method
Details:`Adobe Flash Player/Air Multiple DoS Vulnerabilities - Aug09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800854

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 4865 $

References

CVE: CVE-2009-1863, CVE-2009-1864, CVE-2009-1865, CVE-2009-1866, CVE-2009-1867, ↪CVE-2009-1868, CVE-2009-1869, CVE-2009-1870
BID:35900, 35904, 35906, 35901, 35905, 35902, 35907, 35908
Other:
URL:http://secunia.com/advisories/35948/
URL:http://www.vupen.com/english/advisories/2009/2086
URL:http://www.adobe.com/support/security/bulletins/apsb09-10.html

High (CVSS: 9.3)
NVT: Adobe Flash Player/Air Multiple DoS Vulnerabilities - Aug09 (Linux)

Summary

This host is installed with Adobe Flash Player/Air and is prone to multiple Denial of Service vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to execute arbitrary code, gain elevated privileges, gain knowledge of certain information and conduct clickjacking attacks. Impact Level: System/Application

Solution

Solution type: VendorFix
Update to Adobe Air 1.5.2 or Adobe Flash Player 9.0.246.0 or 10.0.32.18 http://get.adobe.com/air http://www.adobe.com/support/flashplayer/downloads.html

Affected Software/OS

Adobe AIR version prior to 1.5.2 Adobe Flash Player 9 version prior to 9.0.246.0 Adobe Flash Player 10 version prior to 10.0.32.18 on Linux.

Vulnerability Insight

Multiple vulnerabilities which can be to exploited to cause memory corruption, null pointer, privilege escalation, heap-based buffer overflow, local sandbox bypass, and input validation errors when processing specially crafted web pages.

Vulnerability Detection Method

Details:Adobe Flash Player/Air Multiple DoS Vulnerabilities - Aug09 (Linux)
OID:1.3.6.1.4.1.25623.1.0.800854
Version used: $Revision: 4865 $

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2009-1863, CVE-2009-1864, CVE-2009-1865, CVE-2009-1866, CVE-2009-1867,
↪CVE-2009-1868, CVE-2009-1869, CVE-2009-1870
BID:35900, 35904, 35906, 35901, 35905, 35902, 35907, 35908
Other:
URL:http://secunia.com/advisories/35948/
URL:http://www.vupen.com/english/advisories/2009/2086
URL:http://www.adobe.com/support/security/bulletins/apsb09-10.html

High (CVSS: 9.3)
NVT: Adobe Flash Player/Air Multiple Vulnerabilities - August10 (Linux)

Summary
This host is installed with Adobe Flash Player/Air and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary code, cause denial-of-service conditions, or perform click-jacking attacks. Impact Level: Application/System.

Solution
Solution type: VendorFix
Upgrade to Adobe Air 2.0.3 and Adobe Flash Player 9.0.280 or 10.1.82.76 or later For updates refer to http://get.adobe.com/air http://www.adobe.com/support/flashplayer/downloads.html

Affected Software/OS
Adobe AIR version prior to 2.0.3 Adobe Flash Player version before 9.0.280 and 10.x before 10.1.82.76 on Linux

Vulnerability Insight
The flaws are due to memory corruptions and click-jacking issue via unspecified vectors.

Vulnerability Detection Method
Details:Adobe Flash Player/Air Multiple Vulnerabilities - August10 (Linux)
OID:1.3.6.1.4.1.25623.1.0.801256
Version used: $Revision: 5263 $

References
CVE: CVE-2010-0209, CVE-2010-2213, CVE-2010-2215, CVE-2010-2214, CVE-2010-2216
BID:42341
Other:
URL:http://www.adobe.com/support/security/bulletins/apsb10-16.html

High (CVSS: 9.3)
NVT: Adobe Flash Player/Air Multiple Vulnerabilities - August10 (Linux)

Summary
This host is installed with Adobe Flash Player/Air and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary code, cause denial-of-service conditions, or perform click-jacking attacks. Impact Level: Application/System.

Solution
Solution type: VendorFix
Upgrade to Adobe Air 2.0.3 and Adobe Flash Player 9.0.280 or 10.1.82.76 or later For updates refer to http://get.adobe.com/air http://www.adobe.com/support/flashplayer/downloads.html

Affected Software/OS
Adobe AIR version prior to 2.0.3 Adobe Flash Player version before 9.0.280 and 10.x before 10.1.82.76 on Linux

Vulnerability Insight
The flaws are due to memory corruptions and click-jacking issue via unspecified vectors.

Vulnerability Detection Method
Details:`Adobe Flash Player/Air Multiple Vulnerabilities - August10 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.801256
Version used: `$Revision: 5263 $`

References
`CVE: CVE-2010-0209, CVE-2010-2213, CVE-2010-2215, CVE-2010-2214, CVE-2010-2216`
`BID:42341`
`Other:`
`URL:http://www.adobe.com/support/security/bulletins/apsb10-16.html`

High (CVSS: 9.3)
NVT: Adobe Flash Player/Air Multiple Vulnerabilities - June10 (Linux)

Summary
This host is installed with Adobe Flash Player/Air and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow remote attackers to obtain sensitive information or cause a denial of service. Impact Level: Application/System.

Solution
Solution type: VendorFix
Update to Adobe Air2.0.2.12610 or Adobe Flash Player 9.0.277.0 or 10.0.45.2, http://get.adobe.com/air http://www.adobe.com/support/flashplayer/downloads.html

Affected Software/OS
Adobe AIR version prior to 2.0.2.12610, Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64 on Linux.

Vulnerability Insight
The flaws are due to input validation errors, memory corruptions, array indexing, use-after-free, integer and buffer overflows, and invalid pointers when processing malformed Flash content.

Vulnerability Detection Method
Details:`Adobe Flash Player/Air Multiple Vulnerabilities - June10 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.902194
Version used: `$Revision: 5394 $`

References
```
CVE: CVE-2008-4546, CVE-2009-3793, CVE-2010-1297, CVE-2010-2160, CVE-2010-2161,
↪CVE-2010-2162, CVE-2010-2163, CVE-2010-2164, CVE-2010-2165, CVE-2010-2166, CVE
↪-2010-2167, CVE-2010-2169, CVE-2010-2170, CVE-2010-2171, CVE-2010-2172, CVE-20
↪10-2173, CVE-2010-2174, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-
↪2178, CVE-2010-2179, CVE-2010-2180, CVE-2010-2181, CVE-2010-2182, CVE-2010-218
↪3, CVE-2010-2184, CVE-2010-2185, CVE-2010-2186, CVE-2010-2187, CVE-2010-2188,
↪CVE-2010-2189
BID:40759
Other:
  URL:http://www.vupen.com/english/advisories/2010/1421
   URL:http://securitytracker.com/alerts/2010/Jun/1024086.html
   URL:http://www.adobe.com/support/security/bulletins/apsb10-14.html
```

High (CVSS: 9.3)
NVT: Adobe Flash Player/Air Multiple Vulnerabilities - June10 (Linux)

Summary
This host is installed with Adobe Flash Player/Air and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to obtain sensitive information or cause a denial of service. Impact Level: Application/System.

Solution
Solution type: VendorFix
Update to Adobe Air2.0.2.12610 or Adobe Flash Player 9.0.277.0 or 10.0.45.2, http://get.adobe.com/air http://www.adobe.com/support/flashplayer/downloads.html

Affected Software/OS
Adobe AIR version prior to 2.0.2.12610, Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64 on Linux.

Vulnerability Insight
The flaws are due to input validation errors, memory corruptions, array indexing, use-after-free, integer and buffer overflows, and invalid pointers when processing malformed Flash content.

Vulnerability Detection Method
Details:Adobe Flash Player/Air Multiple Vulnerabilities - June10 (Linux)
OID:1.3.6.1.4.1.25623.1.0.902194
Version used: $Revision: 5394 $

References
CVE: CVE-2008-4546, CVE-2009-3793, CVE-2010-1297, CVE-2010-2160, CVE-2010-2161, ↪CVE-2010-2162, CVE-2010-2163, CVE-2010-2164, CVE-2010-2165, CVE-2010-2166, CVE ↪-2010-2167, CVE-2010-2169, CVE-2010-2170, CVE-2010-2171, CVE-2010-2172, CVE-20 ↪10-2173, CVE-2010-2174, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010- ↪2178, CVE-2010-2179, CVE-2010-2180, CVE-2010-2181, CVE-2010-2182, CVE-2010-218 ↪3, CVE-2010-2184, CVE-2010-2185, CVE-2010-2186, CVE-2010-2187, CVE-2010-2188, ↪CVE-2010-2189
BID:40759
Other:
URL:http://www.vupen.com/english/advisories/2010/1421
URL:http://securitytracker.com/alerts/2010/Jun/1024086.html
URL:http://www.adobe.com/support/security/bulletins/apsb10-14.html

High (CVSS: 9.3)
NVT: Adobe Products '.pdf' and '.swf' Code Execution Vulnerability - July09 (Linux)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0 ↪.800108)

Summary
This host is installed with Adobe products and is prone to remote code execution vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause code execution on the affected application.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader/Acrobat version 9.1.3 or later. Upgrade to Adobe Flash Player version 9.0.246.0 or 10.0.32.18 or later. For updates refer to http://www.adobe.com/

Affected Software/OS
Adobe Reader/Acrobat version 9.x to 9.1.2 Adobe Flash Player version 9.x to 9.0.159.0 and 10.x to 10.0.22.87 on Linux.

Vulnerability Insight
- An unspecified error exists in Adobe Flash Player which can be exploited via a specially crafted flash application in a '.pdf' file. - Error occurs in 'authplay.dll' in Adobe Reader/Acrobat whlie processing '.swf' content and can be exploited to execute arbitrary code.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Products '.pdf' and '.swf' Code Execution Vulnerability - July09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900807
Version used: `$Revision: 5055 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
`CVE: CVE-2009-1862`
`BID:35759`
`Other:`
`URL:http://secunia.com/advisories/35948/`
`URL:http://secunia.com/advisories/35949/`
`URL:http://www.kb.cert.org/vuls/id/259425`
`URL:http://www.adobe.com/support/security/advisories/apsa09-03.html`

High (CVSS: 9.3)
NVT: Adobe Products Content Code Execution Vulnerability (Linux)

... continues on next page ...

... continued from previous page ...

Summary
This host has Adobe Acrobat or Adobe Reader or Adobe flash Player installed, and is prone to arbitrary code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code in the context of the user running the affected application.
Impact Level: Application/System

Solution
Solution type: VendorFix
Adobe Flash Player: Upgrade to Adobe Flash Player version 10.1.102.64 or later For details refer, http://www.adobe.com/downloads/
Adobe Reader/Acrobat: Upgrade to Adobe Reader/Acrobat version 9.4.1 or later, For updates refer to http://www.adobe.com/downloads/

Affected Software/OS
Adobe Reader/Acrobat version 9.x to 9.4 on Linux Adobe Flash Player version 10.1.85.3 and prior on Linux

Vulnerability Insight
The flaw is caused by an unspecified error which can be exploited to execute arbitrary code.

Vulnerability Detection Method
Details:`Adobe Products Content Code Execution Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.801478
Version used: `$Revision: 5263 $`

References
```
CVE: CVE-2010-3654
BID:44504
Other:
  URL:http://secunia.com/advisories/41917
   URL:http://www.kb.cert.org/vuls/id/298081
   URL:http://contagiodump.blogspot.com/2010/10/potential-new-adobe-flash-player
↪-zero.html
```

High (CVSS: 9.3)
NVT: Adobe Products Content Code Execution Vulnerability (Linux)

Summary
This host has Adobe Acrobat or Adobe Reader or Adobe flash Player installed, and is prone to arbitrary code execution vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code in the context of the user running the affected application.
Impact Level: Application/System

Solution
Solution type: VendorFix
Adobe Flash Player: Upgrade to Adobe Flash Player version 10.1.102.64 or later For details refer, http://www.adobe.com/downloads/
Adobe Reader/Acrobat: Upgrade to Adobe Reader/Acrobat version 9.4.1 or later, For updates refer to http://www.adobe.com/downloads/

Affected Software/OS
Adobe Reader/Acrobat version 9.x to 9.4 on Linux Adobe Flash Player version 10.1.85.3 and prior on Linux

Vulnerability Insight
The flaw is caused by an unspecified error which can be exploited to execute arbitrary code.

Vulnerability Detection Method
Details:Adobe Products Content Code Execution Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.801478
Version used: $Revision: 5263 $

References
CVE: CVE-2010-3654
BID:44504
Other:
URL:http://secunia.com/advisories/41917
URL:http://www.kb.cert.org/vuls/id/298081
URL:http://contagiodump.blogspot.com/2010/10/potential-new-adobe-flash-player
↪-zero.html

High (CVSS: 9.3)
NVT: Adobe Products Content Code Execution Vulnerability (Windows)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

... continues on next page ...

... continued from previous page ...

Summary
This host has Adobe Acrobat or Adobe Reader or Adobe flash Player installed, and is prone to code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to corrupt memory and execute arbitrary code on the system with elevated privileges.
Impact Level: Application/System

Solution
Solution type: VendorFix
Upgrade to adobe flash version 10.1.85.3 or later and Adobe Reader/Acrobat version 9.4 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Reader/Acrobat version 9.3.4 and prior on Windows. Adobe Flash Player version 10.1.82.76 and prior on Windows

Vulnerability Insight
The flaw is caused by an unspecified error when processing malformed 'Flash' or '3D' and 'Multimedia' content within a PDF document, which could be exploited by attackers to execute arbitrary code by convincing a user to open a specially crafted PDF file.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Products Content Code Execution Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.902303
Version used: `$Revision: 5394 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
`CVE: CVE-2010-2884`
`BID:43205`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/61771`
`URL:http://www.vupen.com/english/advisories/2010/2349`
`URL:http://www.vupen.com/english/advisories/2010/2348`
`URL:http://www.adobe.com/support/security/advisories/apsa10-03.html`

High (CVSS: 9.3)
NVT: Adobe Products Remote Code Execution Vulnerability - jun10 (Linux)

Summary
This host is installed with Adobe products and is prone to remote code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code by tricking a user into opening a specially crafted PDF file.
Impact Level: System/Application

Solution
For Adobe Flash Player, Update to Adobe Flash Player 10.1.53.64 or 9.0.277.0 or later http://www.adobe.com/support/flashplayer/downloads.html
For Adobe Reader Vendor has released a patch for the issue, refer below link, http://www.adobe.com/support/security/advisories/apsa10-01.html For updates refer to http://www.adobe.com/

Affected Software/OS
Adobe Reader version 9.x to 9.3.2 Adobe Flash Player version 9.0.x to 9.0.262 and 10.x through 10.0.45.2

Vulnerability Insight
The flaw is due to a memory corruption error in the 'libauthplay.so.0.0.0' library and 'SWF' file when processing ActionScript Virtual Machine 2 (AVM2) 'newfunction' instructions within Flash content in a PDF document.

Vulnerability Detection Method
Details:`Adobe Products Remote Code Execution Vulnerability - jun10 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.801361
Version used: `$Revision: 5263 $`

References
`CVE: CVE-2010-1297`
`BID:40586`
`Other:`
`URL:http://www.vupen.com/english/advisories/2010/1349`
`URL:http://www.vupen.com/english/advisories/2010/1348`
`URL:http://www.adobe.com/support/security/advisories/apsa10-01.html`

High (CVSS: 9.3)
NVT: Adobe Reader 'printSeps()' Function Heap Corruption Vulnerability

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host is installed with Adobe Reader and is prone to heap corruption Vulnerability

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to crash an affected application or compromise a vulnerable system by tricking a user into opening a specially crafted PDF file.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader/Acrobat version 9.4.1 or later, For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Reader version 8.x to 8.1.7 and 9.x before 9.4.1 on Linux

Vulnerability Insight
This issue is caused by a heap corruption error in the 'EScript.api' plugin when processing the 'printSeps()' function within a PDF document.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader 'printSeps()' Function Heap Corruption Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801546
Version used: $Revision: 5263 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2010-4091
BID:44638
Other:
URL:http://secunia.com/advisories/42095
URL:http://xforce.iss.net/xforce/xfdb/62996
URL:http://www.exploit-db.com/exploits/15419/

... continues on next page ...

... continued from previous page ...

URL:http://www.vupen.com/english/advisories/2010/2890
URL:http://blogs.adobe.com/psirt/2010/11/potential-issue-in-adobe-reader.html

High (CVSS: 9.3)
NVT: Adobe Reader and Acrobat 'CoolType.dll' Memory Corruption Vulnerability

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host is installed with Adobe Reader/Acrobat and is prone to memory corruption and reemote code execution vulnerability

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to crash an affected application or compromise a vulnerable system by tricking a user into opening a specially crafted PDF file.
Impact Level:Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader version 9.4.4 or Acrobat 9.4.4 or 10.0.3 For updates refer to http://www.adobe.com
**** NOTE : No fix available for Adobe Reader X (10.x), vendors are planning to address this issue in next quarterly security update for Adobe Reader. *****

Affected Software/OS
Adobe Reader version prior to 9.4.4 and 10.x to 10.0.1 Adobe Acrobat version prior to 9.4.4 and 10.x to 10.0.2 on windows

Vulnerability Insight
This issue is caused by a memory corruption error in the 'CoolType' library when processing the malformed Flash content within a PDF document.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader and Acrobat 'CoolType.dll' Memory Corruption Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801933
Version used: $Revision: 5424 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2011-0610
BID:47531
Other:
URL:http://www.vupen.com/english/advisories/2011/0923
URL:http://www.adobe.com/support/security/bulletins/apsb11-08.html

High (CVSS: 9.3)
NVT: Adobe Reader and Acrobat Multiple Vulnerabilities February-2011 (Windows)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host is installed with Adobe Reader/Acrobat and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let local attackers to obtain elevated privileges, or by remote attackers to inject scripting code, or execute arbitrary commands by tricking a user into opening a malicious PDF document.
Impact Level:Application

Solution
Solution type: VendorFix
Upgrade to Adobe Acrobat and Reader version 10.0.1, 9.4.2 or 8.2.6. For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Acrobat X version 10.0 Adobe Acrobat version 9.4.1 and prior Adobe Acrobat version 8.2.5 and prior Adobe Reader X version 10.0 Adobe Reader version 9.4.1 and prior Adobe Reader version 8.2.5 and prior

Vulnerability Insight
Multiple flaws are caused by insecure permissions, input validation errors, memory corruptions, and buffer overflow errors when processing malformed contents within a PDF document.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader and Acrobat Multiple Vulnerabilities February-2011 (Windows)
OID:1.3.6.1.4.1.25623.1.0.801844
Version used: $Revision: 5424 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2010-4091, CVE-2011-0562, CVE-2011-0563, CVE-2011-0564, CVE-2011-0565,
↪CVE-2011-0566, CVE-2011-0567, CVE-2011-0568, CVE-2011-0570, CVE-2011-0585, CVE
↪-2011-0586, CVE-2011-0587, CVE-2011-0588, CVE-2011-0589, CVE-2011-0590, CVE-20
↪11-0591, CVE-2011-0592, CVE-2011-0593, CVE-2011-0594, CVE-2011-0595, CVE-2011-
↪0596, CVE-2011-0598, CVE-2011-0599, CVE-2011-0600, CVE-2011-0602, CVE-2011-060
↪3, CVE-2011-0604, CVE-2011-0605, CVE-2011-0606
BID:46146
Other:
URL:http://www.vupen.com/english/advisories/2011/0337
URL:http://www.adobe.com/support/security/bulletins/apsb11-03.html

High (CVSS: 9.3)
NVT: Adobe Reader Denial of Service Vulnerability (May09)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host is installed with Adobe Reader and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let the attacker cause memory corruption or denial of service.
Impact Level: System/Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade Adobe Reader version 9.3.2 or later, For further updates refer, http://www.adobe.com

Affected Software/OS
Adobe Reader version 9.1 and prior on Linux.

Vulnerability Insight
These flaws are due to a memory corruption errors in 'customDictionaryOpen' and 'getAnnots' methods in the JavaScript API while processing malicious PDF files with a long string in the second argument.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Reader Denial of Service Vulnerability (May09)`
OID:1.3.6.1.4.1.25623.1.0.800701
Version used: `$Revision: 4865 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
```
CVE: CVE-2009-1493, CVE-2009-1492
BID:34740, 34736
Other:
  URL:http://secunia.com/advisories/34924
   URL:http://xforce.iss.net/xforce/xfdb/50146
   URL:http://packetstorm.linuxsecurity.com/0904-exploits/spell.txt
```

High (CVSS: 9.3)
NVT: Adobe Reader Multimeda Doc.media.newPlayer Code Execution Vulnerability (Linux)

Product detection result
```
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)
```

Summary
This host is installed with Adobe Reader and is prone to Doc.media.newPlayer Remote Code Execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will let attackers to execute arbitrary code and compromise a user's system.
Impact Level: System

Solution
Solution type: VendorFix
Upgrade Adobe Reader version 9.3.2 or later, For updates refer to http://www.adobe.com
Workaround: Disable JavaScript execution from the Adobe Acrobat/Reader product configuration menu settings.

Affected Software/OS
Adobe Reader version 9.2.0 and prior

Vulnerability Insight
There exists a flaw in the JavaScript module doc.media object while sending a null argument to the newPlayer() method as the exploitation method makes use of a vpointer that has not been initialized.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Reader Multimeda Doc.media.newPlayer Code Execution Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.801095
Version used: `$Revision: 4865 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
```
CVE: CVE-2009-4324
BID:37331
Other:
  URL:http://www.f-secure.com/weblog/archives/00001836.html
   URL:http://extraexploit.blogspot.com/search/label/CVE-2009-4324
   URL:http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20091214
   URL:http://blogs.adobe.com/psirt/2009/12/new_adobe_reader_and_acrobat_v.html
   URL:http://downloads.securityfocus.com/vulnerabilities/exploits/adobe_media_n
↪ewplayer.rb
   URL:http://vrt-sourcefire.blogspot.com/2009/12/adobe-reader-medianewplayer-an
↪alysis.html
```

High (CVSS: 10.0)
NVT: Adobe Reader Multiple BOF Vulnerabilities - Jun09 (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host has Adobe Reader installed, which is prone to multiple buffer overflow vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows remote attackers to execute arbitrary code to cause a stack based overflow via a specially crafted PDF, and could also take complete control of the affected system and cause the application to crash.
Impact Level: System

Solution
Solution type: VendorFix
Upgrade to Adobe Reader version 9.1.2, 8.1.6 and 7.1.3
http://www.adobe.com/support/security/bulletins/apsb09-07.html

Affected Software/OS
Adobe Reader 7 before 7.1.3, 8 before 8.1.6, and 9 before 9.1.2

Vulnerability Insight
Multiple flaws are reported in Adobe Reader. For more information refer, http://www.adobe.com/support/security/bulletins/apsb09-07.html

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader Multiple BOF Vulnerabilities - Jun09 (Linux)
OID:1.3.6.1.4.1.25623.1.0.800586
Version used: $Revision: 4865 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2009-0198, CVE-2009-0509, CVE-2009-0510, CVE-2009-0511, CVE-2009-0512,
↪CVE-2009-1855, CVE-2009-1856, CVE-2009-1857, CVE-2009-0889, CVE-2009-0888, CVE
↪-2009-1858, CVE-2009-1859, CVE-2009-1861, CVE-2009-2028
BID:35274, 35282, 35289, 35291, 35293, 35294, 35295, 35296, 35298, 35299, 35301,

... continues on next page ...

... continued from previous page ...

↪ 35302, 35303
Other:
URL:http://www.adobe.com/support/security/bulletins/apsb09-07.html
URL:http://www.vupen.com/english/advisories/2009/1547
URL:http://secunia.com/advisories/34580

High (CVSS: 9.3)
NVT: Adobe Reader Multiple Unspecified Vulnerabilities -Oct10 (Linux)

Summary
This host is installed with Adobe Reader and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to gain privileges via unknown vectors. Impact Level:Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader version 9.4 or 8.2.5 For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Reader version 8.x before 8.2.5 and 9.x before 9.4 on linux

Vulnerability Insight
An unspecified flaw is present in the application which can be exploited through an unknown attack vectors.

Vulnerability Detection Method
Details:Adobe Reader Multiple Unspecified Vulnerabilities -Oct10 (Linux)
OID:1.3.6.1.4.1.25623.1.0.801525
Version used: $Revision: 5263 $

References
CVE: CVE-2010-2887
BID:43740
Other:
URL:http://secunia.com/advisories/41435/
URL:http://www.vupen.com/english/advisories/2010/2573
URL:http://www.adobe.com/support/security/bulletins/apsb10-21.html

... continues on next page ...

... continued from previous page ...

High (CVSS: 9.3)
NVT: Adobe Reader Multiple Vulnerabilities - Oct09 (Linux)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host has Adobe Reader installed which is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows remote attackers to execute arbitrary code, write arbitrary files or folders to the filesystem, escalate local privileges, or cause a denial of service on an affected system by tricking the user to open a malicious PDF document.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader versions 9.2, 8.1.7, or 7.1.4 or later. For updates refer to http://www.adobe.com/downloads/

Affected Software/OS
Adobe Reader version 7.x before 7.1.4, 8.x before 8.1.7 and 9.x before 9.2 on Linux.

Vulnerability Insight
For more information about the vulnerabilities refer the links mentioned in references.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader Multiple Vulnerabilities - Oct09 (Linux)
OID:1.3.6.1.4.1.25623.1.0.800958
Version used: $Revision: 4865 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2009-2979, CVE-2009-2980, CVE-2009-2981, CVE-2009-2982, CVE-2009-2983,

... continues on next page ...

... continued from previous page ...

```
↪CVE-2009-2984, CVE-2009-2985, CVE-2009-2986, CVE-2009-2987, CVE-2009-2988, CVE
↪-2009-2989, CVE-2009-2990, CVE-2009-2991, CVE-2009-2992, CVE-2009-2993, CVE-20
↪09-2994, CVE-2009-2995, CVE-2009-2996, CVE-2009-2997, CVE-2009-2998, CVE-2009-
↪3458, CVE-2009-3459, CVE-2009-3460, CVE-2009-3462, CVE-2009-3431
BID:36686, 36687, 36688, 36691, 36667, 36690, 36680, 36682, 36693, 36665, 36669,
↪ 36689, 36694, 36681, 36671, 36678, 36677, 36600, 36638, 36696, 35148
Other:
  URL:http://secunia.com/advisories/36983
   URL:http://xforce.iss.net/xforce/xfdb/53691
   URL:http://www.vupen.com/english/advisories/2009/2851
   URL:http://www.vupen.com/english/advisories/2009/2898
   URL:http://securitytracker.com/alerts/2009/Oct/1023007.html
   URL:http://www.adobe.com/support/security/bulletins/apsb09-15.html
```

High (CVSS: 9.3)
NVT: Adobe Reader Multiple Vulnerabilities Feb08 (Linux)

Product detection result

```
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)
```

Summary

This host is installed with Adobe Reader and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to conduct a denial of service and execution of arbitrary code or compromise a user's system.
Impact Level: System/Application

Solution

Solution type: VendorFix
Upgrade to Adobe Reader version 8.1.2 or later. For updates refer, http://www.adobe.com/downloads

Affected Software/OS

Adobe Reader version 8.1.1 and earlier on Linux.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Flaws are due to, - Multiple boundary errors in several unspecified JavaScript methods. - An unspecified insecure JavaScript method in 'EScript.api'. - Untrusted search path error in 'Security Provider' libraries. - An error in insecure JavaScript method 'DOC.print'. - An integer overflow in the 'printSepsWithParams' JavaScript method. - An unspecified error in Javascript API. - Other unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Reader Multiple Vulnerabilities Feb08 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804374
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
```
CVE: CVE-2008-0667, CVE-2007-5666, CVE-2007-5659, CVE-2007-5663, CVE-2008-0726,
↪CVE-2008-0655, CVE-2008-2042
BID:27641
Other:
  URL:http://secunia.com/advisories/28802
   URL:http://www.adobe.com/support/security/advisories/apsa08-01.html
```

High (CVSS: 9.3)
NVT: Adobe Reader Multiple Vulnerabilities February-2011 (Linux)

Product detection result
```
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)
```

Summary
This host is installed with Adobe Reader and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let local attackers to obtain elevated privileges, or by remote attackers to inject scripting code, or execute arbitrary commands by tricking a user into opening a malicious PDF document.
Impact Level:Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to Adobe Reader version 9.4.2 or later, For updates refer to http://www.adobe.com

Affected Software/OS
Adobe Reader 9.4.1 and earlier versions for Linux.

Vulnerability Insight
Multiple flaws are present in Adobe Reader due to insecure permissions, input validation errors, memory corruptions, and buffer overflow errors when processing malformed contents within a PDF document.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Reader Multiple Vulnerabilities February-2011 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.801845
Version used: `$Revision: 5424 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
```
CVE: CVE-2010-4091, CVE-2011-0562, CVE-2011-0563, CVE-2011-0564, CVE-2011-0565,
↪CVE-2011-0566, CVE-2011-0567, CVE-2011-0568, CVE-2011-0570, CVE-2011-0585, CVE
↪-2011-0586, CVE-2011-0587, CVE-2011-0588, CVE-2011-0589, CVE-2011-0590, CVE-20
↪11-0591, CVE-2011-0592, CVE-2011-0593, CVE-2011-0594, CVE-2011-0595, CVE-2011-
↪0596, CVE-2011-0598, CVE-2011-0599, CVE-2011-0600, CVE-2011-0602, CVE-2011-060
↪3, CVE-2011-0604, CVE-2011-0605, CVE-2011-0606
BID:46146
Other:
  URL:http://www.vupen.com/english/advisories/2011/0337
   URL:http://www.adobe.com/support/security/bulletins/apsb11-03.html
```

High (CVSS: 9.3)
NVT: Adobe Reader Multiple Vulnerabilities Jan07 (Linux)

Product detection result
```
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)
```

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with Adobe Reader and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to cause memory corruption, execution of arbitrary code, execution of arbitrary script code in a user's browser session in context of an affected site and conduct cross site request forgery attacks.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader version 7.0.9 or later. For updates refer to http://get.adobe.com/reader

Affected Software/OS
Adobe Reader version 7.0.8 and prior on Linux.

Vulnerability Insight
Flaws exist due to, - Input passed to a hosted PDF file is not properly sanitised by the browser plug-in before being returned to users. - Input passed to a hosted PDF file is not properly handled by the browser plug-in.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Reader Multiple Vulnerabilities Jan07 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804394
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
`CVE: CVE-2006-5857, CVE-2007-0046, CVE-2007-0047, CVE-2007-0044`
`BID:21858, 21981`
`Other:`
`URL:http://secunia.com/advisories/23483`
`URL:http://xforce.iss.net/xforce/xfdb/31266`
`URL:http://www.adobe.com/support/security/bulletins/apsb07-01.html`

High (CVSS: 9.3)
NVT: Adobe Reader/Acrobat Denial of Service Vulnerability (May09)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host is installed with Adobe Reader/Acrobat and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let the attacker cause memory corruption or denial of service.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader/Acrobat version 9.3.2 or later, For further updates refer, http://www.adobe.com

Affected Software/OS
Adobe Reader/Acrobat version 9.1 and prior on Windows.

Vulnerability Insight
This flaw is due to memory corruption error in 'getAnnots' methods in the JavaScript API while processing malicious PDF files that calls this vulnerable method with crafted integer arguments.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader/Acrobat Denial of Service Vulnerability (May09)
OID:1.3.6.1.4.1.25623.1.0.800706
Version used: $Revision: 4865 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2009-1492
BID:34736
Other:
URL:http://secunia.com/advisories/34924
URL:http://xforce.iss.net/xforce/xfdb/50145
URL:http://blogs.adobe.com/psirt/2009/04/update_on_adobe_reader_issue.html

High (CVSS: 10.0)
NVT: Adobe Reader/Acrobat JavaScript Method Handling Vulnerability (Linux)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host has Adobe Reader/Acrobat installed, which is/are prone to Remote Code Execution Vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows remote attackers to execute arbitrary code or an attacker could take complete control of an affected system or cause a denial of service condition.
Impact Level: System

Solution
Solution type: VendorFix
Apply Security Update mentioned in the advisory from the below link, http://www.adobe.com/support/security/bulletins/apsb08-15.html

Affected Software/OS
Adobe Reader version 7.0.9 and prior - Linux(All) Adobe Reader versions 8.0 through 8.1.2 - Linux(All)

Vulnerability Insight
The flaw is due to an input validation error in a JavaScript method, which could allow attackers to execute arbitrary code by tricking a user into opening a specially crafted PDF document.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader/Acrobat JavaScript Method Handling Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.800107
Version used: $Revision: 4218 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2008-2641

. . . continues on next page . . .

... continued from previous page ...

BID:29908
Other:
CB-A:08-0105
URL:http://xforce.iss.net/xforce/xfdb/43307
URL:http://www.frsirt.com/english/advisories/2008/1906/products
URL:http://www.adobe.com/support/security/bulletins/apsb08-15.html

High (CVSS: 9.3)
NVT: Adobe Reader/Acrobat Multimedia Doc.media.newPlayer Code Execution Vulnerability (Windows)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host is installed with Adobe Reader/Acrobat and is prone to Doc.media.newPlayer Remote Code Execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code and compromise a user's system.
Impact Level: System

Solution
Solution type: VendorFix
Adobe Acrobat/Reader version 9.3.2 or later, For updates refer to http://www.adobe.com
Workaround: Disable JavaScript execution from the Adobe Acrobat/Reader product configuration menu settings.

Affected Software/OS
Adobe Acrobat version 9.2.0 and prior. Adobe Acrobat version 9.2.0 and prior.

Vulnerability Insight
There exists a flaw in the JavaScript module doc.media object while sending a null argument to the newPlayer() method as the exploitation method makes use of a vpointer that has not been initialized.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader/Acrobat Multimedia Doc.media.newPlayer Code Execution Vulnerabilit.

... continues on next page ...

... continued from previous page ...

↪..
OID:1.3.6.1.4.1.25623.1.0.901096
Version used: $Revision: 4865 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2009-4324
BID:37331
Other:
URL:http://www.f-secure.com/weblog/archives/00001836.html
URL:http://extraexploit.blogspot.com/search/label/CVE-2009-4324
URL:http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20091214
URL:http://blogs.adobe.com/psirt/2009/12/new_adobe_reader_and_acrobat_v.html
URL:http://downloads.securityfocus.com/vulnerabilities/exploits/adobe_media_n
↪ewplayer.rb
URL:http://vrt-sourcefire.blogspot.com/2009/12/adobe-reader-medianewplayer-an
↪alysis.html

High (CVSS: 10.0)
NVT: Adobe Reader/Acrobat Multiple BOF Vulnerabilities - Jun09 (Windows)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host has Adobe Reader/Acrobat installed, which is/are prone to multiple buffer overflow vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows remote attackers to execute arbitrary code to cause a stack based overflow via a specially crafted PDF, and could also take complete control of the affected system and cause the application to crash.
Impact Level: System

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to Adobe Reader and Acrobat version 9.1.2, 8.1.6 and 7.1.3
http://www.adobe.com/support/security/bulletins/apsb09-07.html

Affected Software/OS
Adobe Reader and Acrobat 7 before 7.1.3, 8 before 8.1.6, and 9 before 9.1.2

Vulnerability Insight
Multiple flaws are reported in Adobe Reader and Acrobat. For more information refer, http://www.adobe.com/support/security/bulletins/apsb09-07.html

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Reader/Acrobat Multiple BOF Vulnerabilities - Jun09 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.800585
Version used: `$Revision: 4865 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
```
CVE: CVE-2009-0198, CVE-2009-0509, CVE-2009-0510, CVE-2009-0511, CVE-2009-0512,
↪CVE-2009-1855, CVE-2009-1856, CVE-2009-1857, CVE-2009-0889, CVE-2009-0888, CVE
↪-2009-1858, CVE-2009-1859, CVE-2009-1861, CVE-2009-2028
BID:35274, 35282, 35289, 35291, 35293, 35294, 35295, 35296, 35298, 35299, 35301,
↪ 35302, 35303
Other:
  URL:http://www.adobe.com/support/security/bulletins/apsb09-07.html
   URL:http://www.vupen.com/english/advisories/2009/1547
   URL:http://secunia.com/advisories/34580
```

High (CVSS: 9.3)
NVT: Adobe Reader/Acrobat Multiple Vulnerabilities - Nov08 (Linux)

Product detection result
```
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)
```

Summary
This host has Adobe Reader/Acrobat installed, which is/are prone to multiple vulnerabilities.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows remote attackers to execute arbitrary code to cause a stack based overflow via a specially crafted PDF, and could also take complete control of the affected system and cause the application to crash.
Impact Level: System

Solution
Solution type: VendorFix
Upgrade to 8.1.3 or higher versions, http://www.adobe.com/products/

Affected Software/OS
Adobe Reader/Acrobat versions 8.1.2 and prior - Linux(All)

Vulnerability Insight
The flaws are due to, - a boundary error when parsing format strings containing a floating point specifier in the util.printf() Javascript function. - improper parsing of type 1 fonts. - bounds checking not being performed after allocating an area of memory.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Reader/Acrobat Multiple Vulnerabilities - Nov08 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800051
Version used: `$Revision: 4218 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
```
CVE: CVE-2008-2992, CVE-2008-2549, CVE-2008-4812, CVE-2008-4813, CVE-2008-4817,
↪CVE-2008-4816, CVE-2008-4814, CVE-2008-4815
BID:30035, 32100
Other:
  URL:http://www.adobe.com/support/security/bulletins/apsb08-19.html
   URL:http://www.coresecurity.com/content/adobe-reader-buffer-overflow
```

High (CVSS: 9.3)
NVT: Adobe Reader/Flash Player Content Code Execution Vulnerability (Linux)

Product detection result
```
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)
```

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Reader/Flash player and is prone to Content Code Execution Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to corrupt memory and execute arbitrary code on the system with elevated privileges.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash version 10.1.85.3 or later and Adobe Reader version 9.4 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Reader version 9.3.4 and before on Linux. Adobe Flash Player version 10.1.82.76 and before on Linux.

Vulnerability Insight
The flaw is caused by an unspecified error when processing malformed 'Flash' or '3D' and 'Multimedia' content within a PDF document, which could be exploited by attackers to execute arbitrary code by convincing a user to open a specially crafted PDF file.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Reader/Flash Player Content Code Execution Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.902304
Version used: `$Revision: 5394 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
`CVE: CVE-2010-2884`
`BID:43205`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/61771`
`URL:http://www.vupen.com/english/advisories/2010/2349`
`URL:http://www.vupen.com/english/advisories/2010/2348`

... continues on next page ...

... continued from previous page ...

URL:http://www.adobe.com/support/security/advisories/apsa10-03.html

High (CVSS: 9.3)
NVT: Adobe Reader/Flash Player Content Code Execution Vulnerability (Linux)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host is installed with Adobe Reader/Flash player and is prone to Content Code Execution Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to corrupt memory and execute arbitrary code on the system with elevated privileges.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Flash version 10.1.85.3 or later and Adobe Reader version 9.4 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Reader version 9.3.4 and before on Linux. Adobe Flash Player version 10.1.82.76 and before on Linux.

Vulnerability Insight
The flaw is caused by an unspecified error when processing malformed 'Flash' or '3D' and 'Multimedia' content within a PDF document, which could be exploited by attackers to execute arbitrary code by convincing a user to open a specially crafted PDF file.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader/Flash Player Content Code Execution Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.902304
Version used: $Revision: 5394 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.800108)

References

```
CVE: CVE-2010-2884
BID:43205
Other:
  URL:http://xforce.iss.net/xforce/xfdb/61771
   URL:http://www.vupen.com/english/advisories/2010/2349
   URL:http://www.vupen.com/english/advisories/2010/2348
   URL:http://www.adobe.com/support/security/advisories/apsa10-03.html
```

High (CVSS: 9.3)
NVT: Adobe Reader/Flash Player Content Code Execution Vulnerability (Linux)

Product detection result

```
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)
```

Summary

This host is installed with Adobe Reader/Flash player and is prone to Content Code Execution Vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will let attackers to corrupt memory and execute arbitrary code on the system with elevated privileges.
Impact Level: System/Application

Solution

Solution type: VendorFix
Upgrade to Adobe Flash version 10.1.85.3 or later and Adobe Reader version 9.4 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS

Adobe Reader version 9.3.4 and before on Linux. Adobe Flash Player version 10.1.82.76 and before on Linux.

Vulnerability Insight

The flaw is caused by an unspecified error when processing malformed 'Flash' or '3D' and 'Multimedia' content within a PDF document, which could be exploited by attackers to execute arbitrary code by convincing a user to open a specially crafted PDF file.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader/Flash Player Content Code Execution Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.902304
Version used: $Revision: 5394 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2010-2884
BID:43205
Other:
URL:http://xforce.iss.net/xforce/xfdb/61771
URL:http://www.vupen.com/english/advisories/2010/2349
URL:http://www.vupen.com/english/advisories/2010/2348
URL:http://www.adobe.com/support/security/advisories/apsa10-03.html

High (CVSS: 10.0)
NVT: Buffer Overflow Vulnerability in Adobe Acrobat and Reader (Windows)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host has Adobe Acrobat or Adobe Reader installed, and is prone to buffer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
This can be exploited to corrupt arbitrary memory via a specially crafted PDF file, related to a non-JavaScript function call and to execute arbitrary code in context of the affected application.
Impact Level: Application/System

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to Reader/Acrobat version 9.1 or 7.1.1 or 8.1.4 or later. For updates refer to http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows

Affected Software/OS
Adobe Reader/Acrobat version 9.x < 9.1, 8.x < 8.1.4, 7.x < 7.1.1 on Windows.

Vulnerability Insight
This issue is due to error in array indexing while processing JBIG2 streams and unspecified vulnerability related to a JavaScript method.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Buffer Overflow Vulnerability in Adobe Acrobat and Reader (Windows)`
OID:1.3.6.1.4.1.25623.1.0.900320
Version used: `$Revision: 5055 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
```
CVE: CVE-2009-0658, CVE-2009-0927, CVE-2009-0193, CVE-2009-0928, CVE-2009-1061,
↪CVE-2009-1062
BID:33751, 34169, 34229
Other:
  URL:http://secunia.com/advisories/33901
   URL:http://www.adobe.com/support/security/bulletins/apsb09-03.html
   URL:http://www.adobe.com/support/security/bulletins/apsb09-04.html
   URL:http://www.adobe.com/support/security/advisories/apsa09-01.html
   URL:http://downloads.securityfocus.com/vulnerabilities/exploits/33751-PoC.pl
```

High (CVSS: 9.3)
NVT: Buffer Overflow Vulnerability in Adobe Reader (Linux)

Product detection result
```
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)
```

Summary
This host has Adobe Reader installed, and is prone to buffer overflow vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Impact
This can be exploited to corrupt arbitrary memory via a specially crafted PDF file, related to a non-JavaScript function call and to execute arbitrary code in context of the affected application.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader version 9.1 or 8.1.4 or later.
http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Unix

Affected Software/OS
Adobe Reader version 9.x < 9.1, 8.x < 8.1.4, 7.x < 7.1.1 on Linux

Vulnerability Insight
This issue is due to error in array indexing while processing JBIG2 streams and unspecified vulnerability related to a JavaScript method.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Buffer Overflow Vulnerability in Adobe Reader (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900321
Version used: `$Revision: 5055 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
`CVE: CVE-2009-0658, CVE-2009-0927`
`BID:33751, 34169, 34229`
`Other:`
`URL:http://secunia.com/advisories/33901`
`URL:http://www.adobe.com/support/security/bulletins/apsb09-03.html`
`URL:http://www.adobe.com/support/security/bulletins/apsb09-04.html`
`URL:http://www.adobe.com/support/security/advisories/apsa09-01.html`
`URL:http://downloads.securityfocus.com/vulnerabilities/exploits/33751-PoC.pl`

High (CVSS: 9.3)
NVT: CTorrent/Enhanced CTorrent Buffer Overflow Vulnerability

Summary

... continues on next page ...

. . . continued from previous page . . .

The host is installed with CTorrent/Enhanced CTorrent and is prone to Buffer Overflow Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue by execute arbitrary code via specially crafted torrent files and can cause denial of service.
Impact Level: System/Application

Solution
Apply the appropriate patch from the below link, http://sourceforge.net/p/dtorrent/bugs/14/ http://sourceforge.net/p/dtorrent/code/HEAD/tree

Affected Software/OS
CTorrent version 1.3.4 on Linux. Enhanced CTorrent version 3.3.2 and prior on Linux.

Vulnerability Insight
A stack based buffer overflow is due to a boundary error within the function 'btFiles::BuildFromMI()' in btfiles.cpp while processing torrent files containing a long path.

Vulnerability Detection Method
Details:`CTorrent/Enhanced CTorrent Buffer Overflow Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.900557
Version used: `$Revision: 5055 $`

References
`CVE: CVE-2009-1759`
`BID:34584`
`Other:`
`URL:http://secunia.com/advisories/34752`
`URL:http://www.milw0rm.com/exploits/8470`
`URL:http://xforce.iss.net/xforce/xfdb/49959`

High (CVSS: 9.3)
NVT: Firefox Multiple Vulnerabilities Dec-09 (Linux)

Summary
The host is installed with Firefox Browser and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow attacker to conduct spoofing attacks, bypass certain security restrictions, manipulate certain data, disclose sensitive information, or compromise a user's system.
Impact Level: Application/System

Solution
Upgrade to Firefox version 3.0.16 http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Firefox version prior to 3.0.16 on Linux.

Vulnerability Insight
For more information about vulnerabilities on Firefox, refer the links mentioned in references.

Vulnerability Detection Method
Details:`Firefox Multiple Vulnerabilities Dec-09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.902005
Version used: `$Revision: 5055 $`

References
```
CVE: CVE-2009-3979, CVE-2009-3981, CVE-2009-3983, CVE-2009-3984, CVE-2009-3985,
↪CVE-2009-3986, CVE-2009-3987
BID:37361, 37363, 37366, 37367, 37370, 37365, 37360
Other:
  URL:http://secunia.com/advisories/37699
   URL:http://www.vupen.com/english/advisories/2009/3547
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-65.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-68.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-69.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-70.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-71.html
```

High (CVSS: 10.0)
NVT: FreeType Multiple Integer Overflow Vulnerability (Linux)

Product detection result
```
cpe:/a:freetype:freetype:2.1.10
Detected by FreeType Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.90062
↪6)
```

Summary
This host has FreeType installed and is prone to Multiple Integer Overflow vulnerability.

Vulnerability Detection Result
```
Installed version: 2.2.1
Fixed version:     2.3.10
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow remote attackers to execute arbitrary code in the context of the affected application.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Apply fix from the below repositories, http://git.savannah.gnu.org/cgit/freetype/freetype2.git/commit/?id=0545ec1
http://git.savannah.gnu.org/cgit/freetype/freetype2.git/commit/?id=79972af4f0485a11dcb19551356c45245749fc5b
http://git.savannah.gnu.org/cgit/freetype/freetype2.git/commit/?id=a18788b14db60ae3673f932249cd02d33a227c4e
*** NOTE : Ignore this warning, if above mentioned patch is applied already. *****

Affected Software/OS
FreeType version 2.3.9 and prior on Linux.

Vulnerability Insight
Multiple integer overflows are due to inadequate validation of data passed into cff/cffload.c, sfnt/ttcmap.c and cff/cffload.c while processing specially crafted fonts.

Vulnerability Detection Method
Details:`FreeType Multiple Integer Overflow Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900631
Version used: `$Revision: 5562 $`

Product Detection Result
Product: `cpe:/a:freetype:freetype:2.1.10`
Method: `FreeType Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900626)

References
`CVE: CVE-2009-0946`
`Other:`
`URL:http://secunia.com/advisories/34723`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=491384`

High (CVSS: 10.0)
NVT: FreeType Multiple Integer Overflow Vulnerability (Linux)

Product detection result
`cpe:/a:freetype:freetype:2.1.10`
`Detected by FreeType Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.90062`
`↪6)`

Summary

... continues on next page ...

... continued from previous page ...

This host has FreeType installed and is prone to Multiple Integer Overflow vulnerability.

Vulnerability Detection Result
`Installed version: 2.1.10`
`Fixed version: 2.3.10`

Impact
Successful exploitation will allow remote attackers to execute arbitrary code in the context of the affected application.
Impact Level: System/Application.

Solution
Solution type: VendorFix
Apply fix from the below repositories, http://git.savannah.gnu.org/cgit/freetype/freetype2.git/commit/?id=0545ec1
http://git.savannah.gnu.org/cgit/freetype/freetype2.git/commit/?id=79972af4f0485a11dcb19551356c45245749fc5b
http://git.savannah.gnu.org/cgit/freetype/freetype2.git/commit/?id=a18788b14db60ae3673f932249cd02d33a227c4e
*** NOTE : Ignore this warning, if above mentioned patch is applied already. *****

Affected Software/OS
FreeType version 2.3.9 and prior on Linux.

Vulnerability Insight
Multiple integer overflows are due to inadequate validation of data passed into cff/cffload.c, sfnt/ttcmap.c and cff/cffload.c while processing specially crafted fonts.

Vulnerability Detection Method
Details:`FreeType Multiple Integer Overflow Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900631
Version used: `$Revision: 5562 $`

Product Detection Result
Product: `cpe:/a:freetype:freetype:2.1.10`
Method: `FreeType Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900626)

References
`CVE: CVE-2009-0946`
`Other:`
`URL:http://secunia.com/advisories/34723`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=491384`

High (CVSS: 10.0)
NVT: GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC)

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote or local attackers to inject shell commmands, allowing local privilege escalation or remote command execution depending on the application vector.
Impact Level: Application

Solution
Apply the patch or upgrade to latest version, For updates refer to http://www.gnu.org/software/bash/

Affected Software/OS
GNU Bash through 4.3

Vulnerability Insight
GNU bash contains a flaw that is triggered when evaluating environment variables passed from another environment. After processing a function definition, bash continues to process trailing strings.

Vulnerability Detection Method
Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell.
Details:`GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC)`
OID:1.3.6.1.4.1.25623.1.0.804490
Version used: `$Revision: 3517 $`

References
`CVE: CVE-2014-6271`
`BID:70103`
`Other:`
`URL:https://access.redhat.com/solutions/1207723`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=1141597`
`URL:https://blogs.akamai.com/2014/09/environment-bashing.html`
`URL:https://community.qualys.com/blogs/securitylabs/2014/09/24/`

High (CVSS: 10.0)
NVT: GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 02

Summary
This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote or local attackers to inject shell commmands, allowing local privilege escalation or remote command execution depending on the application vector.
Impact Level: System/Application

Solution
Apply the patch from the below link, https://ftp.gnu.org/gnu/bash/

Affected Software/OS
GNU Bash through 4.3 bash43-025

Vulnerability Insight
GNU bash contains a flaw that is triggered when evaluating environment variables passed from another environment. After processing a function definition, bash continues to process trailing strings. Incomplete fix to CVE-2014-6271

Vulnerability Detection Method
Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell.
Details:`GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 02`
OID:1.3.6.1.4.1.25623.1.0.802082
Version used: `$Revision: 3517 $`

References
```
CVE: CVE-2014-7169
BID:70137
Other:
  URL:https://shellshocker.net/
   URL:http://www.kb.cert.org/vuls/id/252743
   URL:http://www.openwall.com/lists/oss-security/2014/09/24/32
   URL:https://community.qualys.com/blogs/securitylabs/2014/09/24/bash-remote-co
↪de-execution-vulnerability-cve-2014-6271
```

High (CVSS: 10.0)
NVT: GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 03

Summary
This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow remote or local attackers to inject shell commmands, allowing local privilege escalation or remote command execution depending on the application vector.
Impact Level: System/Application

Solution
Apply the patch from the link below, https://ftp.gnu.org/gnu/bash/

Affected Software/OS
GNU Bash through 4.3 bash43-026

Vulnerability Insight
GNU bash contains a flaw that is triggered when evaluating environment variables passed from another environment. After processing a function definition, bash continues to process trailing strings. Incomplete fix to CVE-2014-7169, CVE-2014-6271, and CVE-2014-6277

Vulnerability Detection Method
Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell.
Details:`GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 03`
OID:1.3.6.1.4.1.25623.1.0.802085
Version used: `$Revision: 3517 $`

References
```
CVE: CVE-2014-6278
BID:70166
Other:
  URL:https://shellshocker.net/
   URL:http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.ht
↪ml
```

High (CVSS: 10.0)
NVT: GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 04

Summary
This host is installed with GNU Bash Shell and is prone to remote command execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote or local attackers to inject shell commmands, allowing local privilege escalation or remote command execution depending on the application vector.
Impact Level: System/Application

... continues on next page ...

... continued from previous page ...

Solution
Apply the patch from the link below, https://ftp.gnu.org/gnu/bash/

Affected Software/OS
GNU Bash through 4.3 bash43-026

Vulnerability Insight
GNU bash contains a flaw that is triggered when evaluating environment variables passed from another environment. After processing a function definition, bash continues to process trailing strings. Incomplete fix to CVE-2014-7169, CVE-2014-6271

Vulnerability Detection Method
Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell.
Details:GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 04
OID:1.3.6.1.4.1.25623.1.0.802086
Version used: $Revision: 3521 $

References
CVE: CVE-2014-6277
BID:70165
Other:
URL:https://shellshocker.net
URL:http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.ht
↪ml

High (CVSS: 10.0)
NVT: GNU Bash Stacked Redirects aka 'redir_stack' Memory Corruption Vulnerability (LSC)

Summary
This host is installed with GNU Bash Shell and is prone to command execution vulnerability.

Vulnerability Detection Result
Result:
redir_stack vulnerable
stderr is not a tty - where are you?
bash: line 1: 10154 Segmentation fault bash -c 'true <<EOF <<EOF <<EOF <<EO
↪F <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF'

Impact
Successful exploitation will allow attackers to corrupt memory to cause a crash or potentially execute arbitrary coommands.
Impact Level: System/Application

Solution
Apply the appropriate patch. For updates refer to refer to http://www.gnu.org/software/bash/

... continues on next page ...

... continued from previous page ...

Affected Software/OS
GNU Bash through 4.3 bash43-026

Vulnerability Insight
GNU bash contains a flaw that is triggered when evaluating untrusted input during stacked redirects handling.

Vulnerability Detection Method
Login to the target machine with ssh credentials and check its possible to execute the commands via GNU bash shell.
Details:`GNU Bash Stacked Redirects aka 'redir_stack' Memory Corruption Vulnerability (L.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.802083
Version used: `$Revision: 3517 $`

References
```
CVE: CVE-2014-7186
BID:70152
Other:
  URL:https://shellshocker.net/
   URL:http://openwall.com/lists/oss-security/2014/09/26/2
   URL:http://openwall.com/lists/oss-security/2014/09/25/32
   URL:http://lcamtuf.blogspot.in/2014/09/bash-bug-apply-unofficial-patch-now.ht
↪ml
```

High (CVSS: 9.3)
NVT: ImageMagick Buffer Overflow Vulnerability (Linux)

Summary
The host is installed with ImageMagick and is prone to Buffer Overflow Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue by executing arbitrary code via a crafted TIFF files in the context of an affected application. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ImageMagick version 6.5.2-9 or later. http://www.imagemagick.org/script/download.php

Affected Software/OS
ImageMagick version prior to 6.5.2-9 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw occurs due to an integer overflow error within the 'XMakeImage()' function in magick/xwindow.c file while processing malformed TIFF files.

Vulnerability Detection Method
Details:`ImageMagick Buffer Overflow Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900565
Version used: `$Revision: 5055 $`

References
`CVE: CVE-2009-1882`
`BID:35111`
`Other:`
`URL:http://secunia.com/advisories/35216/`

High (CVSS: 7.8)
NVT: Linux Kernel Stream Control Transmission Protocol Violation Vulnerability

Summary
This host has Linux Kernel Stream Control Transmission Protocol (SCTP) implementation and is prone to Protocol Violation Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful attacks will result in denial of service via kernel related vectors. Impact Level: System

Solution
Solution type: VendorFix
Upgrade to Linux kernel 2.6.27, or Apply the available patch from below link, http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.27.y.git a=commit h=ba0166708ef4da7eeb61dd92bbba4d5a749d6561
*** NOTE : Ignore this warning if patch is already applied. *****

Affected Software/OS
Linux kernel version before 2.6.27 on all Linux Platforms.

Vulnerability Insight
The issue is with the parameter 'sctp_paramhdr' in sctp_sf_violation_paramlen, sctp_sf_abort_violation, and sctp_make_abort_violation functions of sm.h, sm_make_chunk.c, and sm_statefunc.c files, which has invalid length and incorrect data types in function calls.

Vulnerability Detection Method
Details:`Linux Kernel Stream Control Transmission Protocol Violation Vulnerability`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.800036
Version used: $Revision: 4218 $

References
CVE: CVE-2008-4618
BID:31848
Other:
URL:http://www.openwall.com/lists/oss-security/2008/10/06/1
URL:http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.27

High (CVSS: 10.0)
NVT: Mozilla Firefox 'JavaScript' DoS Vulnerabilities - Sep09 (Linux)

Summary
The host is installed with Firefox browser and is prone to Denial of Service vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
A remote, unauthenticated attacker could execute arbitrary code or cause a vulnerable application to crash. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.14 or 3.5.2 or later http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Mozilla Firefox version prior to 3.0.14 and 3.5 before 3.5.2 on Linux.

Vulnerability Insight
The flaws are due to multiple errors in the browser and JavaScript engines can be exploited to corrupt memory.

Vulnerability Detection Method
Details:Mozilla Firefox 'JavaScript' DoS Vulnerabilities - Sep09 (Linux)
OID:1.3.6.1.4.1.25623.1.0.900849
Version used: $Revision: 5055 $

References
CVE: CVE-2009-3071, CVE-2009-3075
BID:36343
Other:
URL:http://secunia.com/advisories/36671/
URL:http://www.vupen.com/english/advisories/2009/2585
URL:http://www.mozilla.org/security/announce/2009/mfsa2009-47.html

High (CVSS: 7.8)
NVT: Mozilla Firefox Buffer Overflow Vulnerability - July09 (Linux)

Summary
The host is installed with Mozilla Firefox browser and is prone to Buffer Overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful attacks will let attackers to can cause Denial of Service to the legitimate user. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.6.3 or later, For updates refer to http://www.mozilla.com/en-US/firefox/upgrade.html

Affected Software/OS
Firefox version 3.5.1 and prior on Linux

Vulnerability Insight
- A NULL pointer dereference error exists due an unspecified vectors, related to a 'flash bug.' which can cause application crash. - Stack-based buffer overflow error is caused by sending an overly long string argument to the 'document.write' method.

Vulnerability Detection Method
Details:`Mozilla Firefox Buffer Overflow Vulnerability - July09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800847
Version used: `$Revision: 4865 $`

References
`CVE: CVE-2009-2478, CVE-2009-2479`
`BID:35707`
`Other:`
`URL:http://www.milw0rm.com/exploits/9158`
`URL:http://xforce.iss.net/xforce/xfdb/51729`
`URL:https://bugzilla.mozilla.org/show_bug.cgi?id=503286`

High (CVSS: 9.3)
NVT: Mozilla Firefox DoS Vulnerability May-09 (Linux)

Summary
The host is installed with Mozilla Firefox browser and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will let attackers to execute arbitrary code which results in memory corruption. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.10 http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Firefox version prior to 3.0.10 on Linux.

Vulnerability Insight
The flaw is due to error in nsTextFrame::ClearTextRun function in layout/generic/nsTextFrameThebes.cpp via unspecified vectors.

Vulnerability Detection Method
Details:`Mozilla Firefox DoS Vulnerability May-09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800398
Version used: `$Revision: 4865 $`

References
`CVE: CVE-2009-1313`
`BID:34743`
`Other:`
`URL:https://rhn.redhat.com/errata/RHSA-2009-0449.html`
`URL:https://bugzilla.mozilla.org/show_bug.cgi?id=490233`
`URL:http://securitytracker.com/alerts/2009/Apr/1022126.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-23.html`

High (CVSS: 9.3)
NVT: Mozilla Firefox JavaScript Compiler Code Execution Vulnerability (Linux)

Summary
The host is installed with Mozilla Firefox browser and is prone to Remote Code Execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code which results in memory corruption. Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to Firefox version 3.5.1 or later http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Firefox version 3.5 and prior on Linux

Vulnerability Insight
The flaw is due to an error when processing JavaScript code handling 'font' HTML tags and can be exploited to cause memory corruption.

Vulnerability Detection Method
Details:`Mozilla Firefox JavaScript Compiler Code Execution Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800844
Version used: `$Revision: 4865 $`

References
`CVE: CVE-2009-2477`
`BID:35707`
`Other:`
`URL:http://secunia.com/advisories/35798`
`URL:http://www.milw0rm.com/exploits/9137`
`URL:http://www.vupen.com/english/advisories/2009/1868`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-41.html`

High (CVSS: 10.0)
NVT: Mozilla Firefox Multiple Denial Of Service Vulnerabilities - Sep09 (Linux)

Summary
The host is installed with Firefox browser and is prone to multiple Denial of Service vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
A remote, unauthenticated attacker could execute arbitrary code or cause a vulnerable application to crash. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.14 or later http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Mozilla Firefox version prior to 3.0.14 on Linux.

Vulnerability Insight

... continues on next page ...

. . . continued from previous page . . .

- Multiple errors in the browser and JavaScript engines can be exploited to corrupt memory. - The warning dialog displayed when adding or removing security modules via 'pkcs11.addmodule' or 'pkcs11.deletemodule' does not contain enough information. This can be exploited to potentially trick a user into installing a malicious PKCS11 module.

Vulnerability Detection Method
Details:`Mozilla Firefox Multiple Denial Of Service Vulnerabilities - Sep09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900848
Version used: `$Revision: 5055 $`

References
`CVE: CVE-2009-3070, CVE-2009-3074, CVE-2009-3076`
`BID:36343`
`Other:`
`URL:http://secunia.com/advisories/36671/`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-47.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-48.html`

High (CVSS: 10.0)
NVT: Mozilla Firefox Multiple Memory Corruption Vulnerabilities Aug-09 (Linux)

Summary
This host is installed with Mozilla Firefox and is prone to multiple Memory Corruption vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to execute arbitrary code, phishing attack, and can cause Denial of Service. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.13/3.5.2 http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Firefox version before 3.0.13 or 3.5 before 3.5.2 on Linux.

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

Multiple memory corruption due to: - Error in 'js_watch_set()' function in js/src/jsdbgapi.cpp in the JavaScript engine which can be exploited via a crafted '.js' file. - Error in 'libvorbis()' which is used in the application can be exploited via a crafted '.ogg' file. - Error in 'TraceRecorder::snapshot()' function in js/src/jstracer.cpp and other unspecified vectors. - Error in 'window.open()' which fails to sanitise the invalid character in the crafted URL. This allows remote attackers to spoof the address bar, and possibly conduct phishing attacks, via a crafted web page that calls window.open with an invalid character in the URL, makes document.write calls to the resulting object, and then calls the stop method during the loading of the error page.

Vulnerability Detection Method
Details:`Mozilla Firefox Multiple Memory Corruption Vulnerabilities Aug-09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800856
Version used: `$Revision: 4865 $`

References
`CVE: CVE-2009-2662, CVE-2009-2663, CVE-2009-2664, CVE-2009-2654`
`BID:35927, 35803`
`Other:`
`URL:http://secunia.com/advisories/36001/`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-44.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-45.html`

High (CVSS: 10.0)
NVT: Mozilla Firefox Multiple Vulnerabilities - Sep09 (Linux)

Summary
The host is installed with Firefox browser and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
A remote, unauthenticated attacker could execute arbitrary code or cause a vulnerable application to crash. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.14 or 3.5.3 or later http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Mozilla Firefox version prior to 3.0.14 and 3.5 before 3.5.3 on Linux.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

- Multiple errors in the browser and JavaScript engines can be exploited to corrupt memory. - An error exists when processing operations performed on the columns of a XUL tree element. This can be exploited to dereference freed memory via a pointer owned by a column of the XUL tree element. - An error exists when displaying text in the location bar using the default Windows font. This can be exploited to spoof the URL of a trusted site via Unicode characters having a tall line-height. - An error in the implementation of the 'BrowserFeedWriter' object can be exploited to execute arbitrary JavaScript code with chrome privileges.

Vulnerability Detection Method
Details:`Mozilla Firefox Multiple Vulnerabilities - Sep09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900847
Version used: `$Revision: 5055 $`

References
`CVE: CVE-2009-3072, CVE-2009-3077, CVE-2009-3078, CVE-2009-3079`
`BID:36343`
`Other:`
`URL:http://secunia.com/advisories/36671/`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-47.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-49.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-50.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-51.html`

High (CVSS: 10.0)
NVT: Mozilla Firefox Multiple Vulnerabilities December-08 (Linux)

Summary
The host is installed with Mozilla Firefox browser and is prone to multiple vulnerabilities.
Vulnerability: Refer to the reference links for more information on the vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could result in remote arbitrary code execution, bypass security restrictions, sensitive information disclosure, cross site scripting attacks and execute JavaScript code with chrome privileges. Impact Level: System

Solution
Solution type: VendorFix
Upgrade to Firefox version 2.0.0.19 or 3.0.5 http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Firefox version prior to 2.0.0.19 and 3.x to 3.0.4 on Linux.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details:Mozilla Firefox Multiple Vulnerabilities December-08 (Linux)
OID:1.3.6.1.4.1.25623.1.0.800089
Version used: $Revision: 4218 $

References

CVE: CVE-2008-5500, CVE-2008-5501, CVE-2008-5502, CVE-2008-5503, CVE-2008-5504,
↪CVE-2008-5505, CVE-2008-5506, CVE-2008-5507, CVE-2008-5508, CVE-2008-5510, CVE
↪-2008-5511, CVE-2008-5512, CVE-2008-5513
BID:32882
Other:
URL:http://www.mozilla.org/security/announce/2008/mfsa2008-60.html
URL:http://www.mozilla.org/security/announce/2008/mfsa2008-61.html
URL:http://www.mozilla.org/security/announce/2008/mfsa2008-62.html
URL:http://www.mozilla.org/security/announce/2008/mfsa2008-63.html
URL:http://www.mozilla.org/security/announce/2008/mfsa2008-64.html
URL:http://www.mozilla.org/security/announce/2008/mfsa2008-65.html
URL:http://www.mozilla.org/security/announce/2008/mfsa2008-66.html
URL:http://www.mozilla.org/security/announce/2008/mfsa2008-67.html
URL:http://www.mozilla.org/security/announce/2008/mfsa2008-68.html
URL:http://www.mozilla.org/security/announce/2008/mfsa2008-69.html

High (CVSS: 10.0)
NVT: Mozilla Firefox Multiple Vulnerabilities Feb-09 (Linux)

Summary

The host is installed with Mozilla Firefox browser and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could result in bypassing certain security restrictions, information disclosures, JavaScript code executions which can be executed with the privileges of the signed users.
Impact Level: System/Application

Solution

Solution type: VendorFix
Upgrade to Firefox version 3.0.6 http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS

Firefox version 2.x to 3.0.5 on Linux.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws are due to - Cookies marked 'HTTPOnly' are readable by JavaScript through the request calls of XMLHttpRequest methods i.e. XMLHttpRequest.getAllResponseHeaders and XMLHttpRequest.getResponseHeader. - Using local internet shortcut files to access other sites could be bypassed by redirecting to a privileged 'about:' URI e.g. 'about:plugins'. - Chrome XBL methods can be used to execute arbitrary Javascripts within the context of another website through the same origin policy by using 'window.eval' method. - 'components/sessionstore/src/nsSessionStore.js' file does not block the changes of INPUT elements to type='file' during tab restoration. - Error in caching certain HTTP directives which is being ignored by Firefox which can expose sentive data in any shared network.

Vulnerability Detection Method
Details:`Mozilla Firefox Multiple Vulnerabilities Feb-09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900309
Version used: `$Revision: 5055 $`

References
`CVE: CVE-2009-0352, CVE-2009-0353, CVE-2009-0354, CVE-2009-0355, CVE-2009-0356,`
`↪CVE-2009-0357, CVE-2009-0358`
`BID:33598`
`Other:`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-01.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-02.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-03.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-04.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-05.html`
`URL:http://www.mozilla.org/security/announce/2009/mfsa2009-06.html`

High (CVSS: 10.0)
NVT: Mozilla Firefox Multiple Vulnerabilities July-09 (Linux)

Summary
The host is installed with Firefox browser and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attacker to execute arbitrary code, memory corruption, XSS attacks and results in Denial of Service condition. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.12 or 3.5 or later http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Mozilla Firefox version prior to 3.0.12 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple flaws are reported in Firefox, for more information refer below reference links.

Vulnerability Detection Method
Details:`Mozilla Firefox Multiple Vulnerabilities July-09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900397
Version used: `$Revision: 5055 $`

References
```
CVE: CVE-2009-2462, CVE-2009-2463, CVE-2009-2464, CVE-2009-2465, CVE-2009-2466,
↪CVE-2009-2469, CVE-2009-2471, CVE-2009-2472
BID:35765, 35769, 35775, 35770, 35776, 35772, 35766, 35773
Other:
  URL:http://www.vupen.com/english/advisories/2009/1972
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-34.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-37.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-39.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-40.html
```

High (CVSS: 10.0)
NVT: Mozilla Firefox Multiple Vulnerabilities Mar-09 (Linux)

Summary
The host is installed with Mozilla Firefox browser and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attacker execute arbitrary code in the context of an affected web application or can cause URL address bar spoofing attacks or may cause denial of service. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.7 http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Firefox version prior to 3.0.7 on Linux.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws due to - Layout engine error which causes memory corruption and assertion failures. - Layout engine error related to 'nsCSSStyleSheet::GetOwnerNode', events and garage collection which triggers memory corruption. - Layout engine error through a splice of an array that contains 'non-set' elements which causes 'jsarray.cpp' to pass an incorrect argument to the 'ResizeSlots' function which causes application crash. - Vectors related to js_DecompileValueGenerator, jsopcode.cpp, __defineSetter__ and watch which causes a segmentation fault. - Layout engine error in the vector related to 'gczeal'. - Double free vulnerability in Firefox via 'cloned XUL DOM elements' which were linked as a parent and child are not properly handled during garbage collection which causes arbitrary code execution. - 'nsIRDFService' in Firefox allows to bypass the same origin policy and read XML data through another domain by cross-domain redirect. - Error while decoding invisible characters when they are displayed in the location bar which causes incorrect address to be displayed in the URL bar and causes spoofing attacks. - Error in 'window.print' function which causes dos attack via nested calls in the 'onclick' attribute of an 'INPUT' element.

Vulnerability Detection Method
Details:`Mozilla Firefox Multiple Vulnerabilities Mar-09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800362
Version used: `$Revision: 4865 $`

References
```
CVE: CVE-2009-0771, CVE-2009-0772, CVE-2009-0773, CVE-2009-0774, CVE-2009-0775,
↪CVE-2009-0776, CVE-2009-0777, CVE-2009-0821
BID:33969, 33990
Other:
  URL:https://rhn.redhat.com/errata/RHSA-2009-0315.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-07.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-08.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-09.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-11.html
   URL:http://downloads.securityfocus.com/vulnerabilities/exploits/33969.html
```

High (CVSS: 10.0)
NVT: Mozilla Firefox Multiple Vulnerabilities November-08 (Linux)

Summary
The host is installed with Mozilla Firefox browser and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could result in remote arbitrary code execution, bypass security restrictions, spoofing attacks, sensitive information disclosure, and JavaScript code that can be executed with the privileges of the signed user. Impact Level: System

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to Firefox version 2.0.0.18 or 3.0.4 http://www.mozilla.com/en-US/firefox/all-older.html

Affected Software/OS
Firefox version prior to 2.0.0.18 and 3.x to 3.0.3 on Linux.

Vulnerability Detection Method
Details:`Mozilla Firefox Multiple Vulnerabilities November-08 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800058
Version used: `$Revision: 4218 $`

References
```
CVE: CVE-2008-5012, CVE-2008-5013, CVE-2008-5014, CVE-2008-5015, CVE-2008-5016,
↪CVE-2008-5017, CVE-2008-5018, CVE-2008-5019, CVE-2008-5021, CVE-2008-5022, CVE
↪-2008-5023, CVE-2008-5024, CVE-2008-5052, CVE-2008-0017
BID:32281
Other:
  URL:http://www.mozilla.org/security/announce/2008/mfsa2008-47.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-48.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-49.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-50.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-51.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-52.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-53.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-54.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-55.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-56.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-57.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-58.html
```

High (CVSS: 10.0)
NVT: Mozilla Firefox Multiple Vulnerability July-08 (Linux)

Summary
The host is installed with Mozilla Firefox browser, that is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could result in remote arbitrary code execution, spoofing attacks, sensitive information disclosure, and JavaScript code can be executed with the privileges of JAR's signer.
Impact Level: System

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to Firefox version 2.0.0.15 http://www.mozilla.com/en-US/firefox/all-older.html

Affected Software/OS
Firefox version prior to 2.0.0.15 on Linux.

Vulnerability Insight
Issues in browser are due to, - multiple errors in the layout and JavaScript engines that can corrupt memory. - error while handling unprivileged XUL documents that can be exploited to load chrome scripts from a fastload file via <script> elements. - error in mozIJSSubScriptLoader.LoadScript function can bypass XPCNativeWrappers. - error in block re-flow process, which can potentially lead to crash. - error in processing file URLs contained within local directory listings. - errors in the implementation of the Javascript same origin policy - errors in the verification of signed JAR files. - improper implementation of file upload forms result in uploading specially crafted DOM Range and originalTarget elements. - error in Java LiveConnect implementation. - error in processing of Alt Names provided by peer. - error in processing of windows URL shortcuts.

Vulnerability Detection Method
Details:`Mozilla Firefox Multiple Vulnerability July-08 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800020
Version used: `$Revision: 4218 $`

References
```
CVE: CVE-2008-2798, CVE-2008-2799, CVE-2008-2800, CVE-2008-2801, CVE-2008-2802,
↪CVE-2008-2803, CVE-2008-2805, CVE-2008-2806, CVE-2008-2807, CVE-2008-2808, CVE
↪-2008-2809, CVE-2008-2810, CVE-2008-2811
BID:30038
Other:
  CB-A:08-0109
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-21.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-22.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-23.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-24.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-25.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-27.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-28.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-29.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-30.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-31.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-32.html
   URL:http://www.mozilla.org/security/announce/2008/mfsa2008-33.html
```

High (CVSS: 9.3)
NVT: Mozilla Firefox Multiple Vulnerability Jun-09 (Linux)

Summary

... continues on next page ...

... continued from previous page ...

The host is installed with Firefox Browser, which is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could result in remote arbitrary JavaScript code execution, spoofing attacks, sensitive information disclosure, and can cause denial of service. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.11 http://www.mozilla.com/en-US/firefox/all-older.html

Affected Software/OS
Firefox version prior to 3.0.11 on Linux.

Vulnerability Insight
Multiple flaws are reported in Mozilla Firefoz. For more information refer to the reference links.

Vulnerability Detection Method
Details:`Mozilla Firefox Multiple Vulnerability Jun-09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800637
Version used: `$Revision: 4865 $`

References
```
CVE: CVE-2009-1832, CVE-2009-1833, CVE-2009-1834, CVE-2009-1835, CVE-2009-1836,
↪CVE-2009-1837, CVE-2009-1838, CVE-2009-1839, CVE-2009-1840, CVE-2009-1841, CVE
↪-2009-1392, CVE-2009-2043, CVE-2009-2044, CVE-2009-2061, CVE-2009-2065
BID:35326, 35360, 35280
Other:
  URL:http://www.securityfocus.com/archive/1/504214
   URL:http://www.vupen.com/english/advisories/2009/1572
   URL:http://research.microsoft.com/apps/pubs/default.aspx?id=79323
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-24.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-25.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-26.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-27.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-28.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-29.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-30.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-31.html
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-32.html
   URL:http://research.microsoft.com/pubs/79323/pbp-final-with-update.pdf
```

High (CVSS: 9.3)
NVT: Mozilla Firefox PDF JavaScript Restriction Bypass Vulnerability (Linux)

Summary
The host is installed with Mozilla Firefox browser and is prone to PDF Javascript Restriction Bypass Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attacker execute arbitrary codes in the context of the malicious PDF file and execute arbitrary codes into the context of the remote system. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Mozilla Firefox version 3.6.3 or later For updates refer to http://www.mozilla.com/en-US/index.html

Affected Software/OS
Firefox version 3.0.10 and prior on Linux.

Vulnerability Insight
Error while executing DOM calls in response to a javascript: URI in the target attribute of a submit element within a form contained in an inline PDF file which causes bypassing restricted Adobe's JavaScript restrictions.

Vulnerability Detection Method
Details:`Mozilla Firefox PDF JavaScript Restriction Bypass Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900351
Version used: `$Revision: 5055 $`

References
`CVE: CVE-2009-1597`
`Other:`
`URL:http://www.securityfocus.com/archive/1/archive/1/503183/100/0/threaded`
`URL:http://secniche.org/papers/SNS_09_03_PDF_Silent_Form_Re_Purp_Attack.pdf`

High (CVSS: 10.0)
NVT: Mozilla Firefox Remote Code Execution Vulnerabilities July-09 (Linux)

Summary
The host is installed with Firefox browser and is prone to Remote Code Execution vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation could allow remote attacker to execute arbitrary code and results in Denial of Service condition. Impact Level:System/Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.12 or 3.5.1 or later http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Mozilla Firefox version prior to 3.0.12 and 3.5.1 on Linux.

Vulnerability Insight
Error exists when a page contains a Flash object which presents a slow script dialog, and the page is navigated while the dialog is still visible to the user, the Flash plugin is unloaded resulting in a crash due to a call to the deleted object.

Vulnerability Detection Method
Details:`Mozilla Firefox Remote Code Execution Vulnerabilities July-09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900399
Version used: `$Revision: 5055 $`

References
```
CVE: CVE-2009-2467
BID:35767
Other:
  URL:http://secunia.com/advisories/35914
   URL:http://www.vupen.com/english/advisories/2009/1972
   URL:http://www.mozilla.org/security/announce/2009/mfsa2009-35.html
```

High (CVSS: 7.1)
NVT: Mozilla Products 'select()' Denial Of Service Vulnerability (Linux)

Summary
The host is installed with Mozilla Firefox/Seamonkey/Thunderbird and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to cause application crash by consuming the memory. Impact Level: Application

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to Firefox version 2.0.0.19 or 3.0.5 or later http://www.mozilla.com/en-US/firefox/all.html Upgrade to Seamonkey version 1.1.17 or later http://www.seamonkey-project.org/releases/ Apply patch for Thunderbird through above mozilla engine update http://www.mozillamessaging.com/
*** NOTE: Ignore this warning if above mentioned patch is already applied. *****

Affected Software/OS
Seamonkey version prior to 1.1.17 Thunderbird version 2.0.0.22 and prior Firefox version before 2.0.0.19 and 3.x before 3.0.5 on Linux.

Vulnerability Insight
A null pointer dereference error occurs while calling the 'select' method with a large integer, that results in continuous allocation of x+n bytes of memory, exhausting memory after a while.

Vulnerability Detection Method
Details:`Mozilla Products 'select()' Denial Of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800849
Version used: `$Revision: 4869 $`

References
`CVE: CVE-2009-2535, CVE-2009-1692`
`BID:35446`
`Other:`
`URL:http://www.milw0rm.com/exploits/9160`
`URL:http://www.g-sec.lu/one-bug-to-rule-them-all.html`

High (CVSS: 10.0)
NVT: Mozilla Products Multiple Vulnerabilities feb-10 (Linux)

Summary
The host is installed with Mozilla Firefox/Seamonkey and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attackers to potentially execute arbitrary code or compromise a user's system. Impact Level: Application

Solution
Upgrade to Firefox version 3.0.18 or 3.5.8 or later http://www.mozilla.com/en-US/firefox/all.html
Upgrade to Seamonkey version 2.0.3 or later http://www.seamonkey-project.org/releases/

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Seamonkey version prior to 2.0.3 Firefox version 3.0.x before 3.0.18 and 3.5.x before 3.5.8 on Linux.

Vulnerability Insight
- An error exists in the implementation of Web Worker array data types when processing posted messages. This can be exploited to corrupt memory and potentially execute arbitrary code. - An error exists in the implementation of the 'showModalDialog()' function, can be exploited to potentially execute arbitrary JavaScript code in the context of a domain calling the affected function with external parameters. - An error exists when processing SVG documents served with a Content-Type of 'application/octet-stream', can be exploited to execute arbitrary JavaScript code in the context of a domain hosting the SVG document.

Vulnerability Detection Method
Details:`Mozilla Products Multiple Vulnerabilities feb-10 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.902127
Version used: `$Revision: 5394 $`

References
```
CVE: CVE-2009-3988, CVE-2010-0160, CVE-2010-0162
BID:38289, 38285, 38288
Other:
  URL:http://secunia.com/advisories/37242
   URL:http://www.vupen.com/english/advisories/2010/0405
   URL:http://www.mozilla.org/security/announce/2010/mfsa2010-05.html
```

High (CVSS: 7.5)
NVT: Oracle Java SE Multiple Vulnerabilities (Linux)

Product detection result
```
cpe:/a:sun:jre:1.5.0_06
Detected by Sun Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.
↪1.0.800385)
```

Summary
This host is installed with Sun Java SE and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful attacks will allow attackers to affect confidentiality, integrity, and availability via unknown vectors. Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to SE 6 Update 19, JDK and JRE 5.0 Update 24, http://www.oracle.com/technology/deploy/security/critical-patch-updates/javacpumar2010.html

Affected Software/OS
Sun Java SE version 6 Update 18, 5.0 Update 23 on Linux.

Vulnerability Insight
Multiple flaws are due to memory corruptions, buffer overflows, input validation and implementation errors in following components, - HotSpot Server, - Java Runtime Environment, - Java Web Start, - Java Plug-in, - Java 2D, - Sound and - imageIO components

Vulnerability Detection Method
Details:`Oracle Java SE Multiple Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800500
Version used: `$Revision: 5323 $`

Product Detection Result
Product: `cpe:/a:sun:jre:1.5.0_06`
Method: `Sun Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References
```
CVE: CVE-2009-3555, CVE-2010-0082, CVE-2010-0084, CVE-2010-0085, CVE-2010-0087,
↪CVE-2010-0088, CVE-2010-0089, CVE-2010-0090, CVE-2010-0091, CVE-2010-0092, CVE
↪-2010-0093, CVE-2010-0094, CVE-2010-0095, CVE-2010-0837, CVE-2010-0838, CVE-20
↪10-0839, CVE-2010-0840, CVE-2010-0841, CVE-2010-0842, CVE-2010-0843, CVE-2010-
↪0844, CVE-2010-0845, CVE-2010-0846, CVE-2010-0847, CVE-2010-0848, CVE-2010-084
↪9
BID:36935, 39085, 39093, 39094, 39068, 39081, 39095, 39091, 39096, 39090, 39088,
↪ 39075, 39086, 39072, 39069, 39070, 39065, 39067, 39077, 39083, 39084, 39089,
↪39062, 39071, 39078, 39073
Other:
  URL:http://www.vupen.com/english/advisories/2010/0747
   URL:http://securitytracker.com/alerts/2010/Mar/1023774.html
   URL:http://www.oracle.com/technology/deploy/security/critical-patch-updates/j
↪avacpumar2010.html
```

High (CVSS: 7.5)
NVT: Oracle Java SE Multiple Vulnerabilities (Linux)

Product detection result
```
cpe:/a:sun:jre:1.5.0_06
Detected by Sun Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.
↪1.0.800385)
```

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Sun Java SE and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful attacks will allow attackers to affect confidentiality, integrity, and availability via unknown vectors. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to SE 6 Update 19, JDK and JRE 5.0 Update 24, http://www.oracle.com/technology/deploy/security/critical-patch-updates/javacpumar2010.html

Affected Software/OS
Sun Java SE version 6 Update 18, 5.0 Update 23 on Linux.

Vulnerability Insight
Multiple flaws are due to memory corruptions, buffer overflows, input validation and implementation errors in following components, - HotSpot Server, - Java Runtime Environment, - Java Web Start, - Java Plug-in, - Java 2D, - Sound and - imageIO components

Vulnerability Detection Method
Details:`Oracle Java SE Multiple Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800500
Version used: `$Revision: 5323 $`

Product Detection Result
Product: `cpe:/a:sun:jre:1.5.0_06`
Method: `Sun Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References
`CVE: CVE-2009-3555, CVE-2010-0082, CVE-2010-0084, CVE-2010-0085, CVE-2010-0087,`
`↪CVE-2010-0088, CVE-2010-0089, CVE-2010-0090, CVE-2010-0091, CVE-2010-0092, CVE`
`↪-2010-0093, CVE-2010-0094, CVE-2010-0095, CVE-2010-0837, CVE-2010-0838, CVE-20`
`↪10-0839, CVE-2010-0840, CVE-2010-0841, CVE-2010-0842, CVE-2010-0843, CVE-2010-`
`↪0844, CVE-2010-0845, CVE-2010-0846, CVE-2010-0847, CVE-2010-0848, CVE-2010-084`
`↪9`
`BID:36935, 39085, 39093, 39094, 39068, 39081, 39095, 39091, 39096, 39090, 39088,`
`↪ 39075, 39086, 39072, 39069, 39070, 39065, 39067, 39077, 39083, 39084, 39089,`
`↪39062, 39071, 39078, 39073`

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://www.vupen.com/english/advisories/2010/0747
   URL:http://securitytracker.com/alerts/2010/Mar/1023774.html
   URL:http://www.oracle.com/technology/deploy/security/critical-patch-updates/j
↪avacpumar2010.html
```

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Summary
OS End Of Life Detection
The Operating System on the remote host has reached the end of life and should not be used anymore

Vulnerability Detection Result

```
The Operating System (cpe:/o:slackware:slackware_linux:11.0) on the remote host
↪has reached the end of life at 01 Feb 2012
and should not be used anymore.
See https://en.wikipedia.org/wiki/Slackware#Releases for more information.
```

Vulnerability Detection Method
Details:OS End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: $Revision: 5464 $

High (CVSS: 7.5)
NVT: PHP 'libgd' Denial of Service Vulnerability (Linux)

Product detection result

```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     5.6.27/7.0.12
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Update to PHP version 5.6.27 or 7.0.12. For updates refer to http://www.php.net

Affected Software/OS
PHP versions 5.x through 5.6.26 and 7.0.x through 7.0.11 on Linux

Vulnerability Insight
The flaw exist due to an integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP 'libgd' Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809338
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-7568`
`BID:93184`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:http://www.php.net/ChangeLog-7.php`
`URL:http://seclists.org/oss-sec/2016/q3/639`
`URL:https://bugs.php.net/bug.php?id=73003`

High (CVSS: 10.0)
NVT: PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
This host is installed with PHP and is prone to stack buffer overflow vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`

... continues on next page ...

... continued from previous page ...

Fixed version: 5.4.43

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the PHP process. Failed exploit attempts will likely crash the webserver.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 on Linux

Vulnerability Insight
Multiple flaws are due to - Inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script. - Improper validation of file pointer in the 'phar_convert_to_other' function in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (L.
↪..
OID:1.3.6.1.4.1.25623.1.0.807507
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2015-5590, CVE-2015-8838, CVE-2015-5589
BID:75970, 88763, 75974
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:https://bugs.php.net/bug.php?id=69923

High (CVSS: 7.5)
NVT: PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with PHP and is prone to remote code execution vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.4.45`

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely cause a denial-of-service condition.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Linux

Vulnerability Insight
The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Li.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.807505
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2015-6836`
`BID:76644`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:https://bugs.php.net/bug.php?id=70388`

High (CVSS: 7.5)
NVT: PHP 'substr_replace()' Use After Free Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is running PHP and is prone to Use After Free vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.7

Impact
Successful exploitation could allow remote attackers to execute arbitrary code in the context of a web server. Failed attempts will likely result in denial-of-service conditions.
Impact Level: Network

Solution
Solution type: VendorFix
Upgrade to PHP version 5.3.7 or later. For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version 5.3.6 and prior.

Vulnerability Insight
The flaw is due to passing the same variable multiple times to the 'substr_replace()' function, which makes the PHP to use the same pointer in three variables inside the function.

Vulnerability Detection Method
Details:PHP 'substr_replace()' Use After Free Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902356
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2011-1148
BID:46843
Other:
URL:http://bugs.php.net/bug.php?id=54238

... continues on next page ...

... continued from previous page ...

URL:http://openwall.com/lists/oss-security/2011/03/13/3

High (CVSS: 10.0)
NVT: PHP 'type confusion' Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.7

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.7 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.7 on Linux

Vulnerability Insight
The flaw is due to 'type confusion' issues in 'ext/soap/php_encoding.c', 'ext/soap/php_http.c', and 'ext/soap/soap.c' scripts.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'type confusion' Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.808673
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2015-4601
BID:75246
Other:
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 7.5)
NVT: PHP 'var_unserializer' Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.26

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.26, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.26 on Linux

Vulnerability Insight
The flaw is due to improper handling of object-deserialization failures in 'ext/standard/var_unserializer.re' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'var_unserializer' Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.809321
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2016-7411
BID:93009
Other:
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 10.0)
NVT: PHP 5.2.0 and Prior Versions Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
PHP 5.2.0 and prior versions are prone to multiple security vulnerabilities. Successful exploits could allow an attacker to write files in unauthorized locations, cause a denial-of-service condition, and potentially execute code.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5/5.2.1

Solution
Solution type: VendorFix
The vendor has released updates to address these issues. Contact the vendor for details on obtaining and applying the appropriate updates.
Please see the advisories for more information.

Affected Software/OS
These issues are reported to affect PHP 4.4.4 and prior versions in the 4 branch, and 5.2.0 and prior versions in the 5 branch other versions may also be vulnerable.

Vulnerability Detection Method
Details:PHP 5.2.0 and Prior Versions Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100606
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References

... continues on next page ...

... continued from previous page ...

```
CVE: CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, CVE-2007-0909,
↪CVE-2007-0910
BID:22496
Other:
  URL:http://www.securityfocus.com/bid/22496
   URL:http://support.avaya.com/elmodocs2/security/ASA-2007-136.htm
   URL:http://www.php.net/ChangeLog-5.php#5.2.1
   URL:http://www.php.net/releases/5_2_1.php
   URL:http://support.avaya.com/elmodocs2/security/ASA-2007-101.htm
   URL:http://rhn.redhat.com/errata/RHSA-2007-0076.html
   URL:http://rhn.redhat.com/errata/RHSA-2007-0081.html#Red%20Hat%20Linux%20Adva
↪nced%20Workstation%202.1%20for%20the%20Itanium%20Processor
   URL:http://rhn.redhat.com/errata/RHSA-2007-0082.html
   URL:http://rhn.redhat.com/errata/RHSA-2007-0089.html
   URL:http://www.novell.com/linux/security/advisories/2007_44_php.html
```

High (CVSS: 7.5)
NVT: PHP < 5.2.13 Multiple Vulnerabilities

Product detection result

```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary

The remote web server has installed a PHP Version which is prone to Multiple Vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     5.2.13
```

Solution

Solution type: VendorFix

Updates are available. Please see the references for details.

Affected Software/OS

PHP versions prior to 5.2.13 are affected.

Vulnerability Insight

Multiple vulnerabilities exist due to:

1. A 'safe_mode' restriction-bypass vulnerability. Successful exploits could allow an attacker to write session files in arbitrary directions.

2. A 'safe_mode' restriction-bypass vulnerability. Successful exploits could allow an attacker to access files in unauthorized locations or create files in any writable directory.

3. An unspecified security vulnerability that affects LCG entropy.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:PHP < 5.2.13 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100511
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2010-1128, CVE-2010-1129
BID:38182, 38431, 38430
Other:
URL:http://www.securityfocus.com/bid/38182
URL:http://www.securityfocus.com/bid/38431
URL:http://www.securityfocus.com/bid/38430
URL:http://securityreason.com/achievement_securityalert/82
URL:http://www.php.net/releases/5_2_13.php
URL:http://www.php.net
URL:http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/session/sessio
↪n.c?r1=293036&r2=294272
URL:http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/session/sessio
↪n.c?r1=293036&r2=294272

High (CVSS: 7.5)
NVT: PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to arbitrary code execution vulnerability

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.27

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.27, or 5.6.11, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.27 and 5.6.x before 5.6.11 on Linux.

Vulnerability Insight
The flaw is due to Use-after-free vulnerability in the 'spl_ptr_heap_insert' function in 'ext/spl/spl_heap.c'.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808671
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2015-4116`
`BID:75127`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 10.0)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.5.32`

... continues on next page ...

... continued from previous page ...

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.32, or 5.6.18, or 7.0.3, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 on Linux

Vulnerability Insight
The flaw is due an improper handling of zero-length uncompressed data in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808607
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-4342, CVE-2016-2554`
`BID:89154, 83353`
`Other:`
`URL:http://www.php.net/ChangeLog-7.php`
`URL:http://www.openwall.com/lists/oss-security/2016/04/28/2`

High (CVSS: 7.1)
NVT: PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.5.28`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (race condition and heap memory corruption) by leveraging an application that performs many temporary-file accesses.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.28, or 5.6.12, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.28 and 5.6.x before 5.6.12 on Linux

Vulnerability Insight
The flaw is due to script 'main/php_open_temporary_file.c' does not ensure thread safety.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808613
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2015-8878`
`BID:90837`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 7.5)
NVT: PHP Directory Traversal Vulnerability - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`

... continues on next page ...

... continued from previous page ...

↪592)

Summary
This host is installed with PHP and is prone to Directory traversal vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.4.45`

Impact
Successfully exploiting this issue allow remote attackers to read arbitrary empty directories, also to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Linux

Vulnerability Insight
Multiple flaws are due to - An error in the 'ZipArchive::extractTo' function in 'ext/zip/php_zip.c' script. - The xsl_ext_function_php function in ext/xsl/xsltprocessor.c when libxml2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop. - Improper handling of multiple php_var_unserialize calls. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Directory Traversal Vulnerability - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808617
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2014-9767, CVE-2015-6834, CVE-2015-6835, CVE-2015-6837, CVE-2015-6838`
`BID:76652, 76649, 76733, 76734, 76738`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

... continues on next page ...

... continued from previous page ...

URL:http://www.openwall.com/lists/oss-security/2016/03/16/20

High (CVSS: 10.0)
NVT: PHP End Of Life Detection (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
The PHP version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6/7.0

Impact
An end of life version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution
Solution type: VendorFix
Update the PHP version on the remote host to a still supported version.

Affected Software/OS
PHP versions below PHP 5.6

Vulnerability Insight
Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have been reported are fixed and are released in regular point releases.
After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none, depending on the number of reports.
Once the three years of support are completed, the branch reaches its end of life and is no longer supported.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is unsupported.
Details:PHP End Of Life Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.105889
Version used: $Revision: 5580 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
Other:
URL:https://secure.php.net/supported-versions.php

High (CVSS: 10.0)
NVT: PHP Heap-based buffer overflow in 'mbstring' extension

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
The host is running PHP and is prone to Buffer Overflow vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.7

Impact
Successful exploitation could allow attackers to execute arbitrary code via a crafted string containing an HTML entity.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.7 or later, http://www.php.net/downloads.php

Affected Software/OS
PHP version 4.3.0 to 5.2.6 on all running platform.

Vulnerability Insight
The flaw is due to error in mbfilter_htmlent.c file in the mbstring extension. These can be exploited via mb_convert_encoding, mb_check_encoding, mb_convert_variables, and mb_parse_str functions.

Vulnerability Detection Method
Details:PHP Heap-based buffer overflow in 'mbstring' extension
OID:1.3.6.1.4.1.25623.1.0.900185
Version used: $Revision: 4505 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-5557
BID:32948
Other:
URL:http://bugs.php.net/bug.php?id=45722
URL:http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0477.html

High (CVSS: 7.5)
NVT: PHP Imap_Mail_Compose() Function Buffer Overflow Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to a buffer-overflow vulnerability because the application fails to perform boundary checks before copying user-supplied data to insufficiently sized memory buffers.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
An attacker can exploit this issue to execute arbitrary machine code in the context of the affected webserver. Failed exploit attempts will likely crash the webserver, denying service to legitimate users.

Solution
Solution type: VendorFix
The vendor released PHP 4.4.5 and 5.2.1 to address this issue. Please see the references for more information.

Affected Software/OS
This issue affects PHP versions prior to 4.4.5 and 5.2.1.

Vulnerability Detection Method
Details:PHP Imap_Mail_Compose() Function Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100600

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1825
BID:23234
Other:
URL:http://www.securityfocus.com/bid/23234
URL:http://www.php-security.org/MOPB/MOPB-40-2007.html
URL:http://www.php.net/

High (CVSS: 7.5)
NVT: PHP Interruptions and Calltime Arbitrary Code Execution Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to a vulnerability that an attacker could exploit to execute arbitrary code with the privileges of the user running the affected application.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: N/A

Impact
Successful exploits will compromise the application and possibly the computer.

Vulnerability Detection Method
Details:PHP Interruptions and Calltime Arbitrary Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100252
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

References

```
BID:35867
Other:
  URL:http://www.securityfocus.com/bid/35867
   URL:http://www.php.net
   URL:http://www.blackhat.com/presentations/bh-usa-09/ESSER/BHUSA09-Esser-PostE
↪xploitationPHP-PAPER.pdf
```

High (CVSS: 7.5)
NVT: PHP Msg_Receive() Memory Allocation Integer Overflow Vulnerability

Product detection result

```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary

PHP is prone to an integer-overflow vulnerability because it fails to ensure that integer values aren't overrun. Attackers may exploit this issue to cause a buffer overflow and to corrupt process memory.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     4.4.5
```

Impact

Exploiting this issue may allow attackers to execute arbitrary machine code in the context of the affected application. Failed exploit attempts will likely result in a denial-of-service condition.

Solution

Solution type: VendorFix

Reports indicate that the vendor released version 4.4.5 and 5.2.1 to address this issue. Symantec has not confirmed this. Please contact the vendor for information on obtaining and applying fixes.

Affected Software/OS

This issue affects PHP versions prior to 4.4.5 and 5.2.1.

Vulnerability Detection Method

Details:`PHP Msg_Receive() Memory Allocation Integer Overflow Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100592
Version used: `$Revision: 4503 $`

Product Detection Result

Product: `cpe:/a:php:php:4.4.4`

... continues on next page ...

... continued from previous page ...

Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1889
BID:23236
Other:
URL:http://www.securityfocus.com/bid/23236
URL:http://www.php-security.org/MOPB/MOPB-43-2007.html
URL:http://www.php.net/
URL:http://lists.suse.com/archive/suse-security-announce/2007-May/0007.html

High (CVSS: 7.5)
NVT: PHP Multiple Buffer Overflow Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to multiple buffer-overflow vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.9

Impact
Successful exploits may allow attackers to execute arbitrary code in the context of applications using the vulnerable PHP functions. This may result in a compromise of the underlying system. Failed attempts may lead to a denial-of-service condition.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Versions prior to PHP 4.4.9 and PHP 5.2.8 are vulnerable.

Vulnerability Detection Method
Details:PHP Multiple Buffer Overflow Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100583
Version used: $Revision: 4503 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-3659, CVE-2008-3658
BID:30649
Other:
URL:http://www.securityfocus.com/bid/30649
URL:http://www.php.net/ChangeLog-5.php#5.2.8
URL:http://www.php.net/archive/2008.php#id2008-08-07-1
URL:http://www.php.net/
URL:http://support.avaya.com/elmodocs2/security/ASA-2009-161.htm

High (CVSS: 7.5)
NVT: PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.30

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (memory consumption or application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.30, 7.0.15 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.6.30 and 7.0.x before 7.0.15

Vulnerability Insight
Multiple flaws are due to - A integer overflow in the phar_parse_pharfile function in ext/phar/phar.c via a truncated manifest entry in a PHAR archive.

... continues on next page ...

... continued from previous page ...

- A off-by-one error in the phar_parse_pharfile function in ext/phar/phar.c via a crafted PHAR archive with an alias mismatch.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Linux)
OID:1.3.6.1.4.1.25623.1.0.108054
Version used: $Revision: 5132 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-10159, CVE-2016-10160
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php

High (CVSS: 7.5)
NVT: PHP Multiple Double Free Vulnerabilities - Jan15

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.21/5.6.5

Impact
Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.21 or 5.6.5 or later

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions through 5.5.20 and 5.6.x through 5.6.4

Vulnerability Insight
Multiple flaws are due to: - Double free error in the 'zend_ts_hash_graceful_destroy' function in 'zend_ts_hash.c script in the Zend Engine in PHP. - flaw in the 'GetCode_' function in 'gd_gif_in.c' script in GD Graphics Library (LibGD).

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Double Free Vulnerabilities - Jan15`
OID:1.3.6.1.4.1.25623.1.0.805412
Version used: `$Revision: 4498 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2014-9425, CVE-2014-9709
BID:71800, 73306
Other:
  URL:http://securitytracker.com/id/1031479
   URL:https://bugs.php.net/bug.php?id=68676
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Apr16 (Linux)

Product detection result
```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.4.4
Fixed version:     5.5.33
```

Impact
Successfully exploiting this issue allow remote attackers to gain access to potentially sensitive information and conduct a denial of service (memory corruption and application crash).

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.33 or 5.6.19 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.33, and 5.6.x before 5.6.19 on Linux

Vulnerability Insight
Multiple flaws are due to, - A use-after-free error in wddx.c script in the WDDX extension in PHP - An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 01 - Apr16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807807
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-3142, CVE-2016-3141`
`Other:`
`URL:https://bugs.php.net/bug.php?id=71587`
`URL:https://bugs.php.net/bug.php?id=71498`
`URL:https://secure.php.net/ChangeLog-5.php`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Aug16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 4.4.4
Fixed version: 5.5.37

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 on Linux

Vulnerability Insight
Multiple flaws are due to, - The 'php_zip.c' script in the zip extension improperly interacts with the unserialize implementation and garbage collection. - The php_wddx_process_data function in 'wddx.c' script in the WDDX extension mishandled data in a wddx_deserialize call. - The multiple integer overflows in 'mcrypt.c' script in the mcrypt extension. - The double free vulnerability in the '_php_mb_regex_ereg_replace_exec' function in 'php_mbregex.c' script in the mbstring extension. - An integer overflow in the '_gd2GetHeader' function in 'gd_gd2.c' script in the GD Graphics Library. - An integer overflow in the 'gdImageCreate' function in 'gd.c' script in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 01 - Aug16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808788
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-5773, CVE-2016-5772, CVE-2016-5769, CVE-2016-5768, CVE-2016-5766,
↪CVE-2016-5767
BID:91397, 91398, 91399, 91396, 91395
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Jul16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.34

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.34, or 5.6.20, or 7.0.5, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 on Linux

Vulnerability Insight
Multiple flaws are due to, - Multiple integer overflows in the mbfl_strcut function in 'ext/mbstring/libmbfl/mbfl/mbfilter.c' script. - A format string vulnerability in the php_snmp_error function in 'ext/snmp/snmp.c' script. - An improper handling of '\0' characters by the 'phar_analyze_path' function in 'ext/phar/phar.c' script. - An integer overflow in the 'php_raw_url_encode' function in 'ext/standard/url.c' script - An improper handling of continuation-level jumps in 'file_check_mem' function in 'funcs.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 01 - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808199
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2015-8865
BID:85800, 85801, 85802, 85991, 85993
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Mar16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.4.44

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code and to create or overwrite arbitrary files on the system and this may lead to launch further attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 on Linux

Vulnerability Insight
Multiple flaws are due to, - The multiple use-after-free vulnerabilities in SPL unserialize implementation. - An insufficient validation of user supplied input by 'phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 01 - Mar16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.807503
Version used: $Revision: 5083 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2015-6831, CVE-2015-6832, CVE-2015-6833
BID:76737, 76739, 76735
Other:
URL:https://bugs.php.net/bug.php?id=70068
URL:http://www.openwall.com/lists/oss-security/2015/08/19/3

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Aug16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.37

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code or possibly have unspecified other impact via a large integer argument.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.37, or 5.6.23, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.37 and 5.6.x before 5.6.23 on Linux

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws are due to, - The 'spl_array.c' in the SPL extension improperly interacts with the unserialize implementation and garbage collection. - The integer overflow in the 'SplFileObject::fread' function in 'spl_directory.c' in the SPL extension.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 02 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808790
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2016-5771, CVE-2016-5770
BID:91401, 91403
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Jan15

Product detection result
```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary
This host is installed with PHP and is prone to multiple vulnerbilities.

Vulnerability Detection Result
```
Installed version: 4.4.4
Fixed version:     5.6.5
```

Impact
Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.5 or later

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions before 5.6.5

Vulnerability Insight
The flaw is due to a free operation on a stack-based character array by The apprentice_load function in libmagic/apprentice.c in the Fileinfo component.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 02 - Jan15
OID:1.3.6.1.4.1.25623.1.0.805413
Version used: $Revision: 4498 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2014-9426
Other:
URL:https://bugs.php.net/bug.php?id=68665
URL:http://securitytracker.com/id/1031480

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Sep16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.25

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory, to inject arbitrary-type session data by leveraging control of a session name.

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.25, or 7.0.10, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.25 and 7.x before 7.0.10 on Linux

Vulnerability Insight
Multiple flaws are due to - An invalid wddxPacket XML document that is mishandled in a wddx_deserialize call in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_pop_element' function in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_process_data' function in 'ext/wddx/wddx.c' script. - Improper handling of the case of a thumbnail offset that exceeds the file size in 'exif_process_IFD_in_TIFF' function in 'ext/exif/exif.c' script. - Improper validation of gamma values in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - Improper validation of number of colors in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - The script 'ext/session/session.c' skips invalid session names in a way that triggers incorrect parsing. - Improper handling of certain objects in 'ext/standard/var_unserializer.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 02 - Sep16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809319
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2016-7124, CVE-2016-7125, CVE-2016-7126, CVE-2016-7127, CVE-2016-7128,
↪CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132
BID:92756, 92552, 92755, 92757, 92564, 92758
Other:
  URL:http://www.php.net/ChangeLog-7.php
   URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Aug16 (Linux)

Product detection result
```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.5.36`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.36, or 5.6.22, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.36 and 5.6.x before 5.6.22 on Linux

Vulnerability Insight
Multiple flaws are due to, - An integer overflow in the fread function in 'ext/standard/file.c' script. - An integer overflow in the php_html_entities function in 'ext/standard/html.c' script. - An Integer overflow in the php_escape_html_entities_ex function in 'ext/standard/html.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 03 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808792
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-5096 , CVE-2016-5094, CVE-2016-5095`
`BID:90861, 90857, 92144`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)`

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.5.35`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 on Linux.

Vulnerability Insight
The multiple flaws are due to, - An improper validation of TIFF start data in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper validation of IFD sizes in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper construction of spprintf arguments,in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An error in 'grapheme_strpos function' in 'ext/intl/grapheme/grapheme_string.c'. - An error in 'xml_parse_into_struct' function in 'ext/xml/xml.c' script. - The 'bcpowmod' function in 'ext/bcmath/bcmath.c' improperly modifies certain data structures. - An improper validation of input passed to 'bcpowmod' function in 'ext/bcmath/bcmath.c' script. - An error in 'grapheme_strpos' function in ext/intl/grapheme/grapheme_string.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 03 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808603
Version used: `$Revision: 5083 $`

Product Detection Result

. . . continues on next page . . .

... continued from previous page ...

Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References

```
CVE: CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541,
↪CVE-2016-4542, CVE-2016-4543, CVE-2016-4544
BID:89844, 90172, 90173, 90174
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Sep16 (Linux)

Product detection result

```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     5.6.26
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact.
Impact Level: Application

Solution

Solution type: VendorFix
Upgrade to PHP version 5.6.25, or 7.0.10, or later. For updates refer to http://www.php.net

Affected Software/OS

PHP versions prior to 5.6.25 and 7.x before 7.0.10 on Linux

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws are due to, - Use-after-free vulnerability in the 'wddx_stack_destroy' function in 'ext/wddx/wddx.c' script. - Improper varification of a BIT field has the UNSIGNED_FLAG flag in 'ext/mysqlnd/mysqlnd_wireprotocol.c' script. - The ZIP signature-verification feature does not ensure that the uncompressed_filesize field is large enough. - The script 'ext/spl/spl_array.c' proceeds with SplArray unserialization without validating a return value and data type. - The script 'ext/intl/msgformat/msgformat_format.c' does not properly restrict the locale length provided to the Locale class in the ICU library. - An error in the php_wddx_push_element function in ext/wddx/wddx.c.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 03 - Sep16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809317
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417,
↪CVE-2016-7418
BID:93005, 93006, 93004, 93022, 93008, 93007, 93011
Other:
  URL:http://www.php.net/ChangeLog-7.php
   URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 04 - Aug16 (Linux)

Product detection result
```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.4.4
Fixed version:     5.5.36
```

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 on Linux

Vulnerability Insight
Multiple flaws are due to, - The 'get_icu_value_internal' function in 'ext/intl/locale/locale_methods.c' script does not ensure the presence of a '\0' character. - The 'gd_interpolation.c' script in the GD Graphics Library mishandled by the imagescale function.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 04 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808794
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2013-7456, CVE-2016-5093`
`BID:90946, 90859`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:http://www.php.net/ChangeLog-7.php`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 04 - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.4.44`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution to defeat cryptographic protection mechanisms.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 on Linux

Vulnerability Insight
The multiple flaws are due to, - An improper validation of certain Exception objects in 'Zend/zend_exceptions.c' script. - The 'openssl_random_pseudo_bytes' function in 'ext/openssl/openssl.c' incorrectly relies on the deprecated 'RAND_pseudo_bytes' function.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 04 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808604
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2015-8867, CVE-2015-8876, CVE-2015-8873, CVE-2015-8835`
`BID:87481, 90867, 84426, 90712`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.4.42

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to read or write to arbitrary files, also execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Linux

Vulnerability Insight
The multiple flaws are due to, - Improper validation of token extraction for table names, in the php_pgsql_meta_data function in pgsql.c in the PostgreSQL extension. - Integer overflow in the ftp_genlist function in ext/ftp/ftp.c - PHP does not ensure that pathnames lack %00 sequences.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808675
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2015-4644, CVE-2015-4643, CVE-2015-4598

... continues on next page ...

... continued from previous page ...

```
BID:75291, 75292, 75244
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 05 - Jul16 (Linux)

Product detection result

```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     5.5.38
```

Impact

Successfully exploiting this issue may allow attackers to cause a denial of service obtain sensitive information from process memory, or possibly have unspecified other impact.
Impact Level: Application

Solution

Solution type: VendorFix
Upgrade to PHP version 5.5.38, or 5.6.24, or 7.0.9, or later. For updates refer to http://www.php.net

Affected Software/OS

PHP versions before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 on Linux

Vulnerability Insight

Multiple flaws are due to - An integer overflow in the 'php_stream_zip_opener' function in 'ext/zip/zip_stream.c' script. - An integer signedness error in the 'simplestring_addn' function in 'simplestring.c' in xmlrpc-epi. - The 'ext/snmp/snmp.c' script improperly interacts with the unserialize implementation and garbage collection. - The 'locale_accept_from_http' function in 'ext/intl/locale/locale_methods.c' script does not properly restrict calls to the ICU 'uloc_acceptLanguageFromHTTP' function. - An error in the 'exif_process_user_comment' function in 'ext/exif/exif.c' script. - An error in the 'exif_process_IFD_in_MAKERNOTE' function in 'ext/exif/exif.c' script. - The 'ext/session/session.c' does not properly maintain a certain hash data structure. - An integer overflow in the 'virtual_file_ex' function in 'TSRM/tsrm_virtual_cwd.c' script. - An error in the 'php_url_parse_ex' function in 'ext/standard/url.c' script.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 05 - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808634
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-6288, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292,
↪CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297
BID:92111, 92074, 92097, 92073, 92078, 92115, 92094, 92095, 92099
Other:
URL:http://php.net/ChangeLog-5.php
URL:http://php.net/ChangeLog-7.php
URL:http://openwall.com/lists/oss-security/2016/07/24/2

High (CVSS: 10.0)
NVT: PHP Multiple Vulnerabilities - Aug08

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
The host is installed with PHP, that is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.6

Impact
Successful exploitation could result in remote arbitrary code execution, security restrictions bypass, access to restricted files, denial of service.
Impact Level: System

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.6 or above, http://www.php.net/downloads.php

Affected Software/OS

... continues on next page ...

... continued from previous page ...

PHP version prior to 5.2.6

Vulnerability Insight
The flaws are caused by, - an unspecified stack overflow error in FastCGI SAPI (fastcgi.c). - an error during path translation in cgi_main.c. - an error with an unknown impact/attack vectors. - an unspecified error within the processing of incomplete multibyte characters in escapeshellcmd() API function. - error in curl/interface.c in the cURL library(libcurl), which could be exploited by attackers to bypass safe_mode security restrictions. - an error in PCRE. i.e buffer overflow error when handling a character class containing a very large number of characters with codepoints greater than 255(UTF-8 mode).

Vulnerability Detection Method
Details:PHP Multiple Vulnerabilities - Aug08
OID:1.3.6.1.4.1.25623.1.0.800110
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-2050, CVE-2008-2051, CVE-2007-4850, CVE-2008-0599, CVE-2008-0674
BID:29009, 27413, 27786
Other:
CB-A:08-0118
URL:http://pcre.org/changelog.txt
URL:http://www.php.net/ChangeLog-5.php
URL:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0176
URL:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0178
URL:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0086

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - Dec09

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is running PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4

... continues on next page ...

... continued from previous page ...

Fixed version: 5.2.11

Impact
Successful exploitation could allow local attackers to bypass certain security restrictions and cause denial of service.
Impact Level: Network

Solution
Solution type: VendorFix
Upgrade to PHP version 5.3.1, http://www.php.net/downloads.php

Affected Software/OS
PHP version 5.2.10 and prior. PHP version 5.3.x before 5.3.1

Vulnerability Insight
Multiple flaws are due to: - Error in 'proc_open()' function in 'ext/standard/proc_open.c' that does not enforce the 'safe_mode_allowed_env_vars' and 'safe_mode_protected_env_vars' directives, which allows attackers to execute programs with an arbitrary environment via the env parameter. - Error in 'zend_restore_ini_entry_cb()' function in 'zend_ini.c', which allows attackers to obtain sensitive information.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - Dec09
OID:1.3.6.1.4.1.25623.1.0.801060
Version used: $Revision: 4504 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-4018, CVE-2009-2626
BID:37138, 36009
Other:
URL:http://secunia.com/advisories/37482
URL:http://bugs.php.net/bug.php?id=49026
URL:http://securityreason.com/achievement_securityalert/65
URL:http://www.openwall.com/lists/oss-security/2009/11/23/15

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - Sep09

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is running PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.11

Impact
Successful exploitation will allow attackers to spoof certificates and can cause unknown impacts in the context of the web application.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.11 or later http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.2.11

Vulnerability Insight
- An error in 'php_openssl_apply_verification_policy' function that does not properly perform certificate validation. - An input validation error exists in the processing of 'exif' data. - An unspecified error exists related to the sanity check for the color index in the 'imagecolortransparent' function.

Vulnerability Detection Method
Details:PHP Multiple Vulnerabilities - Sep09
OID:1.3.6.1.4.1.25623.1.0.900871
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293
BID:36449
Other:
URL:http://secunia.com/advisories/36791
URL:http://www.php.net/releases/5_2_11.php

... continues on next page ...

... continued from previous page ...

URL:http://www.php.net/ChangeLog-5.php#5.2.11
URL:http://www.openwall.com/lists/oss-security/2009/09/20/1

High (CVSS: 7.5)
NVT: PHP Out of Bounds Read Multiple Vulnerabilities - Jan15

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.4.37/5.5.21/5.6.5

Impact
Successful exploitation will allow remote attackers to obtain sensitive information and trigger unexpected code execution .
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later

Affected Software/OS
PHP versions through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4

Vulnerability Insight
The flaw is due to an out-of-bounds read error in sapi/cgi/cgi_main.c in the CGI component in PHP.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Out of Bounds Read Multiple Vulnerabilities - Jan15
OID:1.3.6.1.4.1.25623.1.0.805414
Version used: $Revision: 4498 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2014-9427
BID:71833
Other:
URL:https://bugs.php.net/bug.php?id=68618

High (CVSS: 7.5)
NVT: PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to remote code execution vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.28/5.4.23/5.5.7

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption).
Impact Level: Application

Solution
Solution type: VendorFix
Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7.

Vulnerability Insight
The flaw is due to a boundary error within the 'asn1_time_to_time_t' function in 'ext/openssl/openssl.c' when parsing X.509 certificates.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13
OID:1.3.6.1.4.1.25623.1.0.804174
Version used: $Revision: 4500 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2013-6420
Other:
URL:http://secunia.com/advisories/56055
URL:http://packetstormsecurity.com/files/124436/PHP-openssl_x509_parse-Memory
↪-Corruption.html

High (CVSS: 7.5)
NVT: PHP Session Data Deserialization Arbitrary Code Execution Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to an arbitrary-code-execution vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
An attacker may exploit this issue to execute arbitrary code within the context of the affected webserver.

Solution
Solution type: VendorFix
Please see the references for more information.

Affected Software/OS
This issue affects PHP 4 versions prior to 4.4.5 and PHP 5 versions prior to 5.2.1.

Vulnerability Detection Method
Details:PHP Session Data Deserialization Arbitrary Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100602
Version used: $Revision: 4503 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References

CVE: CVE-2007-1701, CVE-2007-1700
BID:23120, 23119
Other:
URL:http://www.securityfocus.com/bid/23120
URL:http://www.securityfocus.com/bid/23119
URL:http://www8.itrc.hp.com/service/cki/docDisplay.do?docId=c01056506
URL:http://www.php-security.org/MOPB/MOPB-31-2007.html
URL:http://www.php.net

High (CVSS: 7.5)
NVT: PHP Shared Memory Functions Resource Verification Arbitrary Code Execution Vulnerability

Product detection result

cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary

PHP shared memory functions (shmop) are prone to an arbitrary-code- execution vulnerability.

Vulnerability Detection Result

Installed version: 4.4.4
Fixed version: 4.4.5

Impact

An attacker may exploit this issue to execute arbitrary code within the context of the affected webserver. The attacker may also gain access to RSA keys of the SSL certificate.

Solution

Solution type: VendorFix
The vendor released versions 4.4.5 and 5.2.1 to address this issue. Please see the references for more information.

Affected Software/OS

This issue affects PHP 4 versions prior to 4.4.5 and PHP 5 versions prior to 5.2.1.

Vulnerability Detection Method

Details:PHP Shared Memory Functions Resource Verification Arbitrary Code Execution Vuln.
↪..

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.100605
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1376
BID:22862
Other:
URL:http://www.securityfocus.com/bid/22862
URL:http://www.php-security.org/MOPB/MOPB-15-2007.html
URL:http://www.php.net
URL:http://lists.suse.com/archive/suse-security-announce/2007-May/0007.html

High (CVSS: 7.5)
NVT: PHP sqlite_udf_decode_binary() Function Buffer Overflow Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to a buffer-overflow vulnerability because the application fails to perform boundary checks before copying user-supplied data to insufficiently sized memory buffers.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
An attacker can exploit this issue to execute arbitrary machine code in the context of the affected webserver. Failed exploit attempts will likely crash the webserver, denying service to legitimate users.

Solution
Solution type: VendorFix
Reports indicate that the vendor released versions 4.4.5 and 5.2.1 to address this issue. Please contact the vendor for information on obtaining and applying fixes.
The reporter of this issue indicates that if you are using a shared copy of an external Sqlite library, you will remain vulnerable to this issue, even after upgrading to nonvulnerable versions.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
This issue affects PHP versions prior to 4.4.5 and 5.2.1.

Vulnerability Detection Method
Details:PHP sqlite_udf_decode_binary() Function Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100593
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1888, CVE-2007-1887
BID:23235
Other:
URL:http://www.securityfocus.com/bid/23235
URL:http://www.php.net/ChangeLog-5.php#5.2.3
URL:http://www.php-security.org/MOPB/MOPB-41-2007.html
URL:http://www.php.net/
URL:http://www.securityfocus.com/archive/1/481830

High (CVSS: 7.5)
NVT: PHP Str_Replace() Integer Overflow Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to an integer-overflow vulnerability because it fails to ensure that integer values aren't overrun. Attackers may exploit this issue to cause a buffer-overflow and corrupt process memory.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
Exploiting this issue may allow attackers to execute arbitrary machine code in the context of the affected application. Failed exploit attempts will likely result in a denial-of-service condition.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
The vendor released PHP 4.4.5 and 5.2.1 to address this issue. Please see the references for more information.

Affected Software/OS
This issue affects versions prior to PHP 4.4.5 and 5.2.1.

Vulnerability Detection Method
Details:PHP Str_Replace() Integer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100594
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1885, CVE-2007-1886
BID:23233
Other:
URL:http://www.securityfocus.com/bid/23233
URL:http://www8.itrc.hp.com/service/cki/docDisplay.do?docId=c01056506
URL:http://www.php-security.org/MOPB/MOPB-39-2007.html
URL:http://www.php.net/releases/4_4_5.php
URL:http://www.php.net/releases/5_2_1.php
URL:http://www.php.net/

High (CVSS: 10.0)
NVT: PHP Version < 4.4.5 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 4.4.5 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Update PHP to version 4.4.5 or later.

Vulnerability Detection Method
Details:`PHP Version < 4.4.5 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.110174
Version used: `$Revision: 4506 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2006-4625, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908,
↪CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1286, CVE-2007-1376, CVE
↪-2007-1378, CVE-2007-1379, CVE-2007-1380, CVE-2007-1700, CVE-2007-1701, CVE-20
↪07-1777, CVE-2007-1825, CVE-2007-1835, CVE-2007-1884, CVE-2007-1885, CVE-2007-
↪1886, CVE-2007-1887, CVE-2007-1890
BID:22496, 22805, 22806, 22833, 22862, 23119, 23120, 23169, 23219, 23233, 23234,
↪ 23235, 23236
```

High (CVSS: 7.5)
NVT: PHP Version < 4.4.8 Multiple Vulnerabilities

Product detection result
```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary
PHP version smaller than 4.4.8 suffers from multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.4.4
Fixed version:     4.4.8
```

Solution
Solution type: VendorFix
Update PHP to version 4.4.8 or later.

Vulnerability Detection Method
Details:`PHP Version < 4.4.8 Multiple Vulnerabilities`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.110186
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-3378, CVE-2007-3997, CVE-2007-3799, CVE-2007-4657, CVE-2007-4658,
↪CVE-2008-0145, CVE-2008-2108
BID:24661, 49631

High (CVSS: 7.5)
NVT: PHP Version < 4.4.9 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP < 4.4.9 suffers from multiple vulnerabilities such as buffer overflow and DOS attack.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.9

Solution
Solution type: VendorFix
Upgrade to PHP version 4.4.9 or later.

Vulnerability Detection Method
Details:PHP Version < 4.4.9 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110068
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-4850, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2009-0754

... continues on next page ...

... continued from previous page ...

BID:27413, 30649, 31612, 33542

High (CVSS: 9.3)
NVT: PHP Version < 5.1.2 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
PHP version smaller than 5.1.2 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.1.2

Solution
Solution type: VendorFix
Update PHP to version 5.1.2 or later.

Vulnerability Detection Method
Details:PHP Version < 5.1.2 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110177
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2006-0200, CVE-2006-0207, CVE-2006-0208
BID:16220, 16803

High (CVSS: 10.0)
NVT: PHP Version < 5.2.0 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

Summary
PHP version smaller than 5.2.0 suffers from multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.2.0`

Solution
Solution type: VendorFix
Update PHP to version 5.2.0 or later.

Vulnerability Detection Method
Details:`PHP Version < 5.2.0 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.110173
Version used: `$Revision: 4506 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2006-1015, CVE-2006-1549, CVE-2006-2660, CVE-2006-4486, CVE-2006-4625,`
`↪CVE-2006-4812, CVE-2006-5465, CVE-2006-5706, CVE-2006-7205, CVE-2007-0448, CVE`
`↪-2007-1381, CVE-2007-1584, CVE-2007-1888, CVE-2007-2844, CVE-2007-5424`
`BID:20349, 20879, 49634`

High (CVSS: 10.0)
NVT: PHP Version < 5.2.1 Multiple Vulnerabilities

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
PHP version smaller than 5.2.1 suffers from multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.2.1`

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update PHP to version 5.2.1 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.1 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110175
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2006-6383, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908,
↪CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1376, CVE-2007-1380, CVE
↪-2007-1383, CVE-2007-1452, CVE-2007-1453, CVE-2007-1454, CVE-2007-1700, CVE-20
↪07-1701, CVE-2007-1824, CVE-2007-1825, CVE-2007-1835, CVE-2007-1884, CVE-2007-
↪1885, CVE-2007-1886, CVE-2007-1887, CVE-2007-1889, CVE-2007-1890, CVE-2007-444
↪1, CVE-2007-4586
BID:21508, 22496, 22805, 22806, 22862, 22922, 23119, 23120, 23219, 23233, 23234,
↪ 23235, 23236, 23237, 23238

High (CVSS: 7.5)
NVT: PHP Version < 5.2.11 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.11 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.11

Solution
Solution type: VendorFix
Update PHP to version 5.2.11 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.11 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110176

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018, ↪CVE-2009-5016
BID:36449, 44889

High (CVSS: 9.3)
NVT: PHP Version < 5.2.14 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103 ↪592)

Summary
PHP version smaller than 5.2.14 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.14

Solution
Solution type: VendorFix
Update PHP to version 5.2.14 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.14 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110171
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, ↪CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE

... continues on next page ...

... continued from previous page ...

↪-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3065
BID:38708, 40948, 41991

High (CVSS: 7.8)
NVT: PHP Version < 5.2.2 Vulnerabilitiy

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.2 suffers from a vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.2

Solution
Solution type: VendorFix
Update PHP to version 5.2.2 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.2 Vulnerabilitiy
OID:1.3.6.1.4.1.25623.1.0.110185
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1649
BID:23105

High (CVSS: 7.5)
NVT: PHP Version < 5.2.4 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

... continues on next page ...

... continued from previous page ...

Summary
PHP version smaller than 5.2.4 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.4

Solution
Solution type: VendorFix
Update PHP to version 5.2.4 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.4 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110184
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1413, CVE-2007-2872, CVE-2007-3294, CVE-2007-3378, CVE-2007-3790,
↪CVE-2007-3799, CVE-2007-3806, CVE-2007-4010, CVE-2007-4033, CVE-2007-4255, CVE
↪-2007-4507, CVE-2007-4652, CVE-2007-4658, CVE-2007-4659, CVE-2007-4660, CVE-20
↪07-4661, CVE-2007-4662, CVE-2007-4663
BID:24661, 24261, 24922, 25498

High (CVSS: 9.3)
NVT: PHP Version < 5.2.5 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.5 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.5

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Update PHP to version 5.2.5 or later.

Vulnerability Detection Method
Details:`PHP Version < 5.2.5 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.110179
Version used: `$Revision: 4506 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2007-3996, CVE-2007-4782, CVE-2007-4783, CVE-2007-4784, CVE-2007-4825,`
`↪CVE-2007-4840, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE`
`↪-2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2008-2107, CVE-2008-2108, CVE-20`
`↪08-4107`
`BID:26403`

High (CVSS: 10.0)
NVT: PHP Version < 5.2.6 Multiple Vulnerabilities

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
PHP version smaller than 5.2.6 suffers from multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.2.6`

Solution
Solution type: VendorFix
Update PHP to version 5.2.6 or later.

Vulnerability Detection Method
Details:`PHP Version < 5.2.6 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.110183

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-4850, CVE-2007-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, ↪CVE-2008-2051
BID:27413, 28392, 29009

High (CVSS: 10.0)
NVT: PHP Version < 5.2.7 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103 ↪592)

Summary
PHP version smaller than 5.2.7 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.7

Solution
Solution type: VendorFix
Update PHP to version 5.2.7 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.7 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110172
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, ↪CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE

... continues on next page ...

... continued from previous page ...

↪-2008-5658
BID:29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948

High (CVSS: 7.5)
NVT: PHP Version < 5.2.8 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.8 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.8

Solution
Solution type: VendorFix
Update PHP to version 5.2.8 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.8 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110180
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-5814, CVE-2008-5844
BID:32673

High (CVSS: 7.5)
NVT: PHP Version < 5.3.1 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

... continues on next page ...

... continued from previous page ...

Summary
PHP version smaller than 5.3.1 suffers from multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.3.1`

Solution
Solution type: VendorFix
Update PHP to version 5.3.1 or later.

Vulnerability Detection Method
Details:`PHP Version < 5.3.1 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.110178
Version used: `$Revision: 4506 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2009-3557, CVE-2009-3559, CVE-2009-4017, CVE-2009-4018, CVE-2010-1128`
`BID:36554, 36555, 37079, 37138`

High (CVSS: 9.3)
NVT: PHP Version < 5.3.3 Multiple Vulnerabilities

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
PHP version smaller than 5.3.3 suffers from multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.3.3`

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Update PHP to version 5.3.3 or later.

Vulnerability Detection Method
Details:PHP Version < 5.3.3 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110182
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,
↪CVE-2010-1917, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE
↪-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3062, CVE-20
↪10-3063, CVE-2010-3064, CVE-2010-3065
BID:38708, 40461, 40948, 41991

High (CVSS: 7.5)
NVT: PHP Versions Prior to 5.3.1 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to multiple security vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.2

Impact
Some of these issues may be exploited to bypass security restrictions and create arbitrary files or cause denial-of-service conditions. The impact of the other issues has not been specified.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
These issues affect PHP versions prior to 5.3.1.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:PHP Versions Prior to 5.3.1 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100359
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
BID:37079
Other:
URL:http://www.securityfocus.com/bid/37079
URL:http://securityreason.com/securityalert/6601
URL:http://securityreason.com/securityalert/6600
URL:http://www.php.net/releases/5_3_1.php
URL:http://www.php.net/
URL:http://seclists.org/fulldisclosure/2009/Nov/228
URL:http://www.securityfocus.com/archive/1/507982

High (CVSS: 7.5)
NVT: PHP Zip_Entry_Read() Integer Overflow Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to an integer-overflow vulnerability because it fails to ensure that integer values aren't overrun. Attackers may exploit this issue to cause a heap-based buffer overflow.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
Exploiting this issue may allow attackers to execute arbitrary machine code in the context of the affected application. Failed exploit attempts will likely result in a denial-of-service condition.

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Reports indicate that PHP 4.4.5 addresses this issue. Please contact the vendor for more information.

Affected Software/OS
This issue affects versions prior to PHP 4.4.5.

Vulnerability Detection Method
Details:PHP Zip_Entry_Read() Integer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100601
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1777
BID:23169
Other:
URL:http://www.securityfocus.com/bid/23169
URL:http://www.php-security.org/MOPB/MOPB-35-2007.html
URL:http://www.php.net/

High (CVSS: 10.0)
NVT: ProFTPD Multiple Remote Vulnerabilities

Product detection result
cpe:/a:proftpd:proftpd:1.3.0
Detected by ProFTPD Server Version Detection (Local) (OID: 1.3.6.1.4.1.25623.1.0
↪.900506)

Summary
The host is running ProFTPD and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.3.0
Fixed version: 1.3.3c

Impact
Successful exploitation may allow execution of arbitrary code or cause a denial-of-service.
Impact Level: Application

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to ProFTPD version 1.3.3c or later, For updates refer to http://www.proftpd.org/

Affected Software/OS
ProFTPD versions prior to 1.3.3c

Vulnerability Insight
- An input validation error within the 'mod_site_misc' module can be exploited to create and delete directories, create symlinks, and change the time of files located outside a writable directory. - A logic error within the 'pr_netio_telnet_gets()' function in 'src/netio.c' when processing user input containing the Telnet IAC escape sequence can be exploited to cause a stack-based buffer overflow by sending specially crafted input to the FTP or FTPS service.

Vulnerability Detection Method
Details:`ProFTPD Multiple Remote Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.801639
Version used: `$Revision: 4774 $`

Product Detection Result
Product: `cpe:/a:proftpd:proftpd:1.3.0`
Method: `ProFTPD Server Version Detection (Local)`
OID: 1.3.6.1.4.1.25623.1.0.900506)

References
```
CVE: CVE-2010-3867, CVE-2010-4221
BID:44562
Other:
  URL:http://secunia.com/advisories/42052
   URL:http://bugs.proftpd.org/show_bug.cgi?id=3519
   URL:http://bugs.proftpd.org/show_bug.cgi?id=3521
   URL:http://www.zerodayinitiative.com/advisories/ZDI-10-229/
```

High (CVSS: 9.0)
NVT: ProFTPD Prior To 1.3.3g Use-After-Free Remote Code Execution Vulnerability

Product detection result
```
cpe:/a:proftpd:proftpd:1.3.0
Detected by ProFTPD Server Version Detection (Local) (OID: 1.3.6.1.4.1.25623.1.0
↪.900506)
```

Summary
ProFTPD is prone to a remote code-execution vulnerability.

Vulnerability Detection Result
```
Installed version: 1.3.0
```

... continues on next page ...

... continued from previous page ...

Fixed version: 1.3.3g

Impact
Successful exploits will allow attackers to execute arbitrary code within the context of the application. Failed exploit attempts will result in a denial-of-service condition.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
ProFTPD prior to 1.3.3g are vulnerable.

Vulnerability Detection Method
Details:ProFTPD Prior To 1.3.3g Use-After-Free Remote Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103331
Version used: $Revision: 4774 $

Product Detection Result
Product: cpe:/a:proftpd:proftpd:1.3.0
Method: ProFTPD Server Version Detection (Local)
OID: 1.3.6.1.4.1.25623.1.0.900506)

References
CVE: CVE-2011-4130
BID:50631
Other:
URL:http://www.securityfocus.com/bid/50631
URL:http://bugs.proftpd.org/show_bug.cgi?id=3711
URL:http://www.proftpd.org
URL:http://www.zerodayinitiative.com/advisories/ZDI-11-328/

High (CVSS: 8.5)
NVT: QEMU VNC Server Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:qemu:qemu:0.9.0
Detected by QEMU Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.900969)

Summary
This host is running QEMU and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Installed version: 0.9.0

... continues on next page ...

... continued from previous page ...

Fixed version: 0.11.0

Impact
Successful exploitation will let the attacker cause memory or CPU consumption, resulting in Denial of Service condition.
Impact level: Application/System

Solution
Solution type: VendorFix
Apply the available patches. http://git.savannah.gnu.org/cgit/qemu.git/commit/?id=753b405331
http://git.savannah.gnu.org/cgit/qemu.git/commit/?id=198a0039c5
**** NOTE: Ignore this warning if the above mentioned patches is already applied. *****

Affected Software/OS
QEMU version 0.10.6 and prior on Linux.

Vulnerability Insight
Multiple use-after-free errors occur in 'vnc.c' in VNC server while processing malicious 'SetEncodings' messages sent via VNC client.

Vulnerability Detection Method
Details:QEMU VNC Server Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.900970
Version used: $Revision: 5122 $

Product Detection Result
Product: cpe:/a:qemu:qemu:0.9.0
Method: QEMU Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.900969)

References
CVE: CVE-2009-3616
BID:36716
Other:
URL:https://bugzilla.redhat.com/show_bug.cgi?id=505641
URL:http://www.openwall.com/lists/oss-security/2009/10/16/8

High (CVSS: 8.5)
NVT: QEMU VNC Server Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:qemu:qemu:0.9.0
Detected by QEMU Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.900969)

... continues on next page ...

... continued from previous page ...

Summary
This host is running QEMU and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
`Installed version: 0.9.0`
`Fixed version: 0.11.0`

Impact
Successful exploitation will let the attacker cause memory or CPU consumption, resulting in Denial of Service condition.
Impact level: Application/System

Solution
Solution type: VendorFix
Apply the available patches. http://git.savannah.gnu.org/cgit/qemu.git/commit/?id=753b405331
http://git.savannah.gnu.org/cgit/qemu.git/commit/?id=198a0039c5
**** NOTE: Ignore this warning if the above mentioned patches is already applied. *****

Affected Software/OS
QEMU version 0.10.6 and prior on Linux.

Vulnerability Insight
Multiple use-after-free errors occur in 'vnc.c' in VNC server while processing malicious 'SetEncodings' messages sent via VNC client.

Vulnerability Detection Method
Details:`QEMU VNC Server Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900970
Version used: `$Revision: 5122 $`

Product Detection Result
Product: `cpe:/a:qemu:qemu:0.9.0`
Method: `QEMU Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900969)

References
`CVE: CVE-2009-3616`
`BID:36716`
`Other:`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=505641`
`URL:http://www.openwall.com/lists/oss-security/2009/10/16/8`

High (CVSS: 10.0)
NVT: Samba End Of Life Detection

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:samba:samba:3.0.14
Detected by Samba Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800403)

Summary
The PostgreSQL version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The Samba version has reached the end of life.
Installed version: 3.0.14
EOL version: 3.0
EOL date: 2009-08-05

Impact
An end of life version of PostgreSQL is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution
Solution type: VendorFix
Update the PostgreSQL version on the remote host to a still supported version.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is unsupported.
Details:Samba End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.140159
Version used: $Revision: 5300 $

Product Detection Result
Product: cpe:/a:samba:samba:3.0.14
Method: Samba Version Detection
OID: 1.3.6.1.4.1.25623.1.0.800403)

References
Other:
URL:https://wiki.samba.org/index.php/Samba_Release_Planning

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2006-335-02 proftpd

Summary
The remote host is missing an update as announced via advisory SSA:2006-335-02.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`Package proftpd-1.3.0a-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-335-02

Vulnerability Insight
New proftpd packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-335-02 proftpd`
OID:1.3.6.1.4.1.25623.1.0.57703
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2006-5815, CVE-2006-6170, CVE-2006-6171`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2006-335-02 proftpd

Summary
The remote host is missing an update as announced via advisory SSA:2006-335-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-335-02

Vulnerability Insight
New proftpd packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-335-02 proftpd`
OID:1.3.6.1.4.1.25623.1.0.57703
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2006-5815, CVE-2006-6170, CVE-2006-6171`

High (CVSS: 7.8)
NVT: Slackware Advisory SSA:2007-026-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2007-026-01.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-026-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix denial of service security issues.
Versions of bind-9.2.x older than bind-9.2.8, and versions of bind-9.3.x older than 9.3.4 can be made to crash with malformed local or remote data.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-026-01 bind`
OID:1.3.6.1.4.1.25623.1.0.57834
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2007-0493, CVE-2007-0494`

High (CVSS: 7.8)
NVT: Slackware Advisory SSA:2007-026-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2007-026-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-026-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix denial of service security issues.
Versions of bind-9.2.x older than bind-9.2.8, and versions of bind-9.3.x older than 9.3.4 can be made to crash with malformed local or remote data.

Vulnerability Detection Method
. . . continues on next page . . .

... continued from previous page ...

Details:Slackware Advisory SSA:2007-026-01 bind
OID:1.3.6.1.4.1.25623.1.0.57834
Version used: $Revision: 5999 $

References
CVE: CVE-2007-0493, CVE-2007-0494

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2007-038-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2007-038-01.

Vulnerability Detection Result
Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-038-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, and 11.0 to fix a denial-of-service security issue.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2007-038-01 samba
OID:1.3.6.1.4.1.25623.1.0.58026
Version used: $Revision: 5912 $

References
CVE: CVE-2007-0452, CVE-2007-0453, CVE-2007-0454

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2007-038-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2007-038-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-038-01

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, and 11.0 to fix a denial-of-service security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-038-01 samba`
OID:1.3.6.1.4.1.25623.1.0.58026
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2007-0452, CVE-2007-0453, CVE-2007-0454`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2007-066-02 x11

Summary
The remote host is missing an update as announced via advisory SSA:2007-066-02.

Vulnerability Detection Result
`Package x11-6.9.0-i486-11 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-066-02

Vulnerability Insight
New x11 packages are available for Slackware 10.2 and 11.0.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-066-02 x11`
OID:1.3.6.1.4.1.25623.1.0.58133
Version used: `$Revision: 5888 $`

References
`CVE: CVE-2006-6101, CVE-2006-6102, CVE-2006-6103`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2007-066-02 x11

Summary
The remote host is missing an update as announced via advisory SSA:2007-066-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-066-02

Vulnerability Insight
New x11 packages are available for Slackware 10.2 and 11.0.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-066-02 x11`
OID:1.3.6.1.4.1.25623.1.0.58133
Version used: `$Revision: 5888 $`

References
`CVE: CVE-2006-6101, CVE-2006-6102, CVE-2006-6103`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2007-085-02 libwpd

Summary
The remote host is missing an update as announced via advisory SSA:2007-085-02.

Vulnerability Detection Result
`Package libwpd-0.8.6-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-085-02

Vulnerability Insight
New libwpd packages are available for Slackware 10.2, 11.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-085-02 libwpd`
OID:1.3.6.1.4.1.25623.1.0.58164
Version used: `$Revision: 6032 $`

References
`CVE: CVE-2007-0002`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2007-085-02 libwpd

Summary
The remote host is missing an update as announced via advisory SSA:2007-085-02.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-085-02

Vulnerability Insight
New libwpd packages are available for Slackware 10.2, 11.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-085-02 libwpd`
OID:1.3.6.1.4.1.25623.1.0.58164
Version used: `$Revision: 6032 $`

References
`CVE: CVE-2007-0002`

High (CVSS: 8.5)
NVT: Slackware Advisory SSA:2007-109-01 freetype

Summary
The remote host is missing an update as announced via advisory SSA:2007-109-01.

Vulnerability Detection Result
`Package fontconfig-2.2.3-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-109-01

Vulnerability Insight
New x11 and/or freetype and fontconfig packages are available for Slackware 10.1, 10.2, 11.0, and -current to fix security issues in freetype. Freetype was packaged with X11 prior to Slackware version 11.0.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-109-01 freetype`
OID:1.3.6.1.4.1.25623.1.0.58229
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2007-1351`

High (CVSS: 8.5)
NVT: Slackware Advisory SSA:2007-109-01 freetype

Summary
The remote host is missing an update as announced via advisory SSA:2007-109-01.

Vulnerability Detection Result
`Package freetype-1.3.1-i386-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-109-01

Vulnerability Insight
New x11 and/or freetype and fontconfig packages are available for Slackware 10.1, 10.2, 11.0, and -current to fix security issues in freetype. Freetype was packaged with X11 prior to Slackware version 11.0.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-109-01 freetype`
OID:1.3.6.1.4.1.25623.1.0.58229
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2007-1351`

High (CVSS: 8.5)
NVT: Slackware Advisory SSA:2007-109-01 freetype

Summary
The remote host is missing an update as announced via advisory SSA:2007-109-01.

Vulnerability Detection Result
`Package x11-6.9.0-i486-11 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-109-01

Vulnerability Insight
New x11 and/or freetype and fontconfig packages are available for Slackware 10.1, 10.2, 11.0, and -current to fix security issues in freetype. Freetype was packaged with X11 prior to Slackware version 11.0.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-109-01 freetype`
OID:1.3.6.1.4.1.25623.1.0.58229

. . . continues on next page . . .

... continued from previous page ...

Version used: `$Revision: 5988 $`

References
`CVE: CVE-2007-1351`

High (CVSS: 8.5)
NVT: Slackware Advisory SSA:2007-109-01 freetype

Summary
The remote host is missing an update as announced via advisory SSA:2007-109-01.

Vulnerability Detection Result
`Package x11-devel-6.9.0-i486-3 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-109-01

Vulnerability Insight
New x11 and/or freetype and fontconfig packages are available for Slackware 10.1, 10.2, 11.0, and -current to fix security issues in freetype. Freetype was packaged with X11 prior to Slackware version 11.0.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-109-01 freetype`
OID:1.3.6.1.4.1.25623.1.0.58229
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2007-1351`

High (CVSS: 8.5)
NVT: Slackware Advisory SSA:2007-109-01 freetype

Summary
The remote host is missing an update as announced via advisory SSA:2007-109-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-109-01

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

New x11 and/or freetype and fontconfig packages are available for Slackware 10.1, 10.2, 11.0, and -current to fix security issues in freetype. Freetype was packaged with X11 prior to Slackware version 11.0.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-109-01 freetype`
OID:1.3.6.1.4.1.25623.1.0.58229
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2007-1351`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2007-134-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2007-134-01.

Vulnerability Detection Result
`Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-134-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-134-01 samba`
OID:1.3.6.1.4.1.25623.1.0.58282
Version used: `$Revision: 5958 $`

References
`CVE: CVE-2007-2444, CVE-2007-2446, CVE-2007-2447`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2007-134-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2007-134-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-134-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-134-01 samba`
OID:1.3.6.1.4.1.25623.1.0.58282
Version used: `$Revision: 5958 $`

References
`CVE: CVE-2007-2444, CVE-2007-2446, CVE-2007-2447`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2007-255-01 openssh

Summary
The remote host is missing an update as announced via advisory SSA:2007-255-01.

Vulnerability Detection Result
`Package openssh-4.4p1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-255-01

Vulnerability Insight
New openssh packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 to fix a possible security issue. This version should also provide increased performance with certain ciphers.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-255-01 openssh`
OID:1.3.6.1.4.1.25623.1.0.59014
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2007-4752`

... continues on next page ...

... continued from previous page ...

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2007-255-01 openssh

Summary
The remote host is missing an update as announced via advisory SSA:2007-255-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-255-01

Vulnerability Insight
New openssh packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 to fix a possible security issue. This version should also provide increased performance with certain ciphers.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-255-01 openssh`
OID:1.3.6.1.4.1.25623.1.0.59014
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2007-4752`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2007-305-01 cups

Summary
The remote host is missing an update as announced via advisory SSA:2007-305-01.

Vulnerability Detection Result
`Package cups-1.1.23-i486-4 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-305-01

Vulnerability Insight
CUPS was found to contain errors in ipp.c which could allow a remote attacker to crash CUPS, resulting in a denial of service. If you use CUPS, it is recommended to update to the latest package for your version of Slackware.
The latest cups package is available for Slackware -current, and patched packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 that fix the problems.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-305-01 cups`
OID:1.3.6.1.4.1.25623.1.0.59022
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2007-4351`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2007-305-01 cups

Summary
The remote host is missing an update as announced via advisory SSA:2007-305-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-305-01

Vulnerability Insight
CUPS was found to contain errors in ipp.c which could allow a remote attacker to crash CUPS, resulting in a denial of service. If you use CUPS, it is recommended to update to the latest package for your version of Slackware.
The latest cups package is available for Slackware -current, and patched packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 that fix the problems.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-305-01 cups`
OID:1.3.6.1.4.1.25623.1.0.59022
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2007-4351`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2007-316-01 xpdf/poppler/koffice/kdegraphics

Summary
The remote host is missing an update as announced via advisory SSA:2007-316-01.

Vulnerability Detection Result
`Package kdegraphics-3.5.4-i486-1 is installed which is known to be vulnerable.`

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-316-01

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current. New poppler packages are available for Slackware 12.0 and -current. New koffice packages are available for Slackware 11.0, 12.0, and -current. New kdegraphics packages are available for Slackware 10.2, 11.0, 12.0, and -current.
These updated packages address similar bugs which could be used to crash applications linked with poppler or that use code from xpdf through the use of a malformed PDF document. It is possible that a maliciously crafted document could cause code to be executed in the context of the user running the application processing the PDF.
This advisoriy cover the bugs: http://www.kde.org/info/security/advisory-20071107-1.txt

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-316-01 xpdf/poppler/koffice/kdegraphics`
OID:1.3.6.1.4.1.25623.1.0.59020
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2007-3387, CVE-2007-4352, CVE-2007-5392, CVE-2007-5393`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2007-316-01 xpdf/poppler/koffice/kdegraphics

Summary
The remote host is missing an update as announced via advisory SSA:2007-316-01.

Vulnerability Detection Result
`Package xpdf-3.01-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-316-01

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current. New poppler packages are available for Slackware 12.0 and -current. New koffice packages are available for Slackware 11.0, 12.0, and -current. New kdegraphics packages are available for Slackware 10.2, 11.0, 12.0, and -current.
These updated packages address similar bugs which could be used to crash applications linked with poppler or that use code from xpdf through the use of a malformed PDF document. It is possible that a maliciously crafted document could cause code to be executed in the context of the user running the application processing the PDF.

. . . continues on next page . . .

... continued from previous page ...

This advisoriy cover the bugs: http://www.kde.org/info/security/advisory-20071107-1.txt

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-316-01 xpdf/poppler/koffice/kdegraphics`
OID:1.3.6.1.4.1.25623.1.0.59020
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2007-3387, CVE-2007-4352, CVE-2007-5392, CVE-2007-5393`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2007-316-01 xpdf/poppler/koffice/kdegraphics

Summary
The remote host is missing an update as announced via advisory SSA:2007-316-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-316-01

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current. New poppler packages are available for Slackware 12.0 and -current. New koffice packages are available for Slackware 11.0, 12.0, and -current. New kdegraphics packages are available for Slackware 10.2, 11.0, 12.0, and -current.
These updated packages address similar bugs which could be used to crash applications linked with poppler or that use code from xpdf through the use of a malformed PDF document. It is possible that a maliciously crafted document could cause code to be executed in the context of the user running the application processing the PDF.
This advisoriy cover the bugs: http://www.kde.org/info/security/advisory-20071107-1.txt

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-316-01 xpdf/poppler/koffice/kdegraphics`
OID:1.3.6.1.4.1.25623.1.0.59020
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2007-3387, CVE-2007-4352, CVE-2007-5392, CVE-2007-5393`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2007-320-01 samba

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update as announced via advisory SSA:2007-320-01.

Vulnerability Detection Result
`Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-320-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-320-01 samba`
OID:1.3.6.1.4.1.25623.1.0.59026
Version used: `$Revision: 5888 $`

References
`CVE: CVE-2007-4572, CVE-2007-5398`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2007-320-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2007-320-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-320-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-320-01 samba`
OID:1.3.6.1.4.1.25623.1.0.59026
Version used: `$Revision: 5888 $`

References
`CVE: CVE-2007-4572, CVE-2007-5398`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2007-344-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2007-344-01.

Vulnerability Detection Result
`Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-344-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix a security issue. A boundary failure in GETDC mailslot processing can result in a buffer overrun leading to possible code execution.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-344-01 samba`
OID:1.3.6.1.4.1.25623.1.0.60018
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2007-6015`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2007-344-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2007-344-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-344-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix a security issue. A boundary failure in GETDC mailslot processing can result in a buffer overrun leading to possible code execution.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-344-01 samba`
OID:1.3.6.1.4.1.25623.1.0.60018

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 5956 $`

References
`CVE: CVE-2007-6015`

High (CVSS: 7.1)
NVT: Slackware Advisory SSA:2007-348-01 mysql

Summary
The remote host is missing an update as announced via advisory SSA:2007-348-01.

Vulnerability Detection Result
`Package mysql-5.0.24a-i486-1kjz is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-348-01

Vulnerability Insight
New mysql packages are available for Slackware 11.0, 12.0, and -current to fix bugs and security issues.
More information (including about a potentially incompatible change) may be found in the release notes:
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-cs-5-0-51.html

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-348-01 mysql`
OID:1.3.6.1.4.1.25623.1.0.60017
Version used: `$Revision: 5950 $`

References
`CVE: CVE-2007-3781, CVE-2007-5925, CVE-2007-5969`

High (CVSS: 7.1)
NVT: Slackware Advisory SSA:2007-348-01 mysql

Summary
The remote host is missing an update as announced via advisory SSA:2007-348-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-348-01

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Insight
New mysql packages are available for Slackware 11.0, 12.0, and -current to fix bugs and security issues.
More information (including about a potentially incompatible change) may be found in the release notes:
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-cs-5-0-51.html

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-348-01 mysql`
OID:1.3.6.1.4.1.25623.1.0.60017
Version used: `$Revision: 5950 $`

References
`CVE: CVE-2007-3781, CVE-2007-5925, CVE-2007-5969`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2008-098-01 m4

Summary
The remote host is missing an update as announced via advisory SSA:2008-098-01.

Vulnerability Detection Result
`Package m4-1.4.6-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-098-01

Vulnerability Insight
New m4 packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-098-01 m4`
OID:1.3.6.1.4.1.25623.1.0.60827
Version used: `$Revision: 5977 $`

References
`CVE: CVE-2008-1687, CVE-2008-1688`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2008-098-01 m4

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update as announced via advisory SSA:2008-098-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-098-01

Vulnerability Insight
New m4 packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-098-01 m4`
OID:1.3.6.1.4.1.25623.1.0.60827
Version used: `$Revision: 5977 $`

References
`CVE: CVE-2008-1687, CVE-2008-1688`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2008-119-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2008-119-01.

Vulnerability Detection Result
`Package libpng-1.2.12-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-119-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix a security issue.
Additional information can be found in the libpng source, or in this file on the libpng FTP site:
ftp://ftp.simplesystems.org/pub/libpng/png/src/libpng-1.2.27-README.txt

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-119-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.60875
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2008-1382`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2008-119-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2008-119-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-119-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix a security issue.
Additional information can be found in the libpng source, or in this file on the libpng FTP site: ftp://ftp.simplesystems.org/pub/libpng/png/src/libpng-1.2.27-README.txt

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-119-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.60875
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2008-1382`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2008-148-01 rdesktop

Summary
The remote host is missing an update as announced via advisory SSA:2008-148-01.

Vulnerability Detection Result
`Package rdesktop-1.5.0-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-148-01

Vulnerability Insight
New rdesktop packages are available for Slackware 11.0, 12.0, 12.1, and -current to fix a security issue caused by using rdesktop to connect to a malicious or compromised RDP server.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-148-01 rdesktop`
OID:1.3.6.1.4.1.25623.1.0.61459

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 5940 $`

References
`CVE: CVE-2008-1801`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2008-148-01 rdesktop

Summary
The remote host is missing an update as announced via advisory SSA:2008-148-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-148-01

Vulnerability Insight
New rdesktop packages are available for Slackware 11.0, 12.0, 12.1, and -current to fix a security issue caused by using rdesktop to connect to a malicious or compromised RDP server.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-148-01 rdesktop`
OID:1.3.6.1.4.1.25623.1.0.61459
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2008-1801`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2008-149-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2008-149-01.

Vulnerability Detection Result
`Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-149-01

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, and -current to fix a security issue:
'Specifically crafted SMB responses can result in a heap overflow in the Samba client code. Because the server process, smbd, can itself act as a client during operations such as printer notification and domain authentication, this issue affects both Samba client and server installations.'
This flaw affects Samba versions from 3.0.0 through 3.0.29.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-149-01 samba`
OID:1.3.6.1.4.1.25623.1.0.61458
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2008-1105`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2008-149-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2008-149-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-149-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, and -current to fix a security issue:
'Specifically crafted SMB responses can result in a heap overflow in the Samba client code. Because the server process, smbd, can itself act as a client during operations such as printer notification and domain authentication, this issue affects both Samba client and server installations.'
This flaw affects Samba versions from 3.0.0 through 3.0.29.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-149-01 samba`
OID:1.3.6.1.4.1.25623.1.0.61458
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2008-1105`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2008-179-01 ruby

Summary
The remote host is missing an update as announced via advisory SSA:2008-179-01.

Vulnerability Detection Result
`Package ruby-1.8.4-i686-1kjz is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-179-01

Vulnerability Insight
New ruby packages are available for Slackware 11.0, 12.0, 12.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-179-01 ruby`
OID:1.3.6.1.4.1.25623.1.0.61462
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2008-2662, CVE-2008-2663, CVE-2008-2664, CVE-2008-2725, CVE-2008-2726`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2008-179-01 ruby

Summary
The remote host is missing an update as announced via advisory SSA:2008-179-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-179-01

Vulnerability Insight
New ruby packages are available for Slackware 11.0, 12.0, 12.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-179-01 ruby`
OID:1.3.6.1.4.1.25623.1.0.61462
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2008-2662, CVE-2008-2663, CVE-2008-2664, CVE-2008-2725, CVE-2008-2726`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2008-217-01 python

Summary
The remote host is missing an update as announced via advisory SSA:2008-217-01.

Vulnerability Detection Result
`Package python-2.4.3-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-217-01

Vulnerability Insight
New python packages are available for Slackware 10.1, 10.2, 11.0, 12.0, 12.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-217-01 python`
OID:1.3.6.1.4.1.25623.1.0.61467
Version used: `$Revision: 5950 $`

References
`CVE: CVE-2008-1679, CVE-2008-1721, CVE-2008-2315, CVE-2008-2316, CVE-2008-3142,`
`↪CVE-2008-3144`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2008-217-01 python

Summary
The remote host is missing an update as announced via advisory SSA:2008-217-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-217-01

Vulnerability Insight
New python packages are available for Slackware 10.1, 10.2, 11.0, 12.0, 12.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-217-01 python`
OID:1.3.6.1.4.1.25623.1.0.61467
Version used: `$Revision: 5950 $`

. . . continues on next page . . .

... continued from previous page ...

References
CVE: CVE-2008-1679, CVE-2008-1721, CVE-2008-2315, CVE-2008-2316, CVE-2008-3142, ↪CVE-2008-3144

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2008-324-01 libxml2

Summary
The remote host is missing an update as announced via advisory SSA:2008-324-01.

Vulnerability Detection Result
Package libxml2-2.6.26-i486-1 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-324-01

Vulnerability Insight
New libxml2 packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, and -current to fix security issues including a denial or service or the possible execution of arbitrary code if untrusted XML is processed.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2008-324-01 libxml2
OID:1.3.6.1.4.1.25623.1.0.61909
Version used: $Revision: 5999 $

References
CVE: CVE-2008-4225, CVE-2008-4226

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2008-324-01 libxml2

Summary
The remote host is missing an update as announced via advisory SSA:2008-324-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-324-01

Vulnerability Insight

... continues on next page ...

. . . continued from previous page . . .

New libxml2 packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, and -current to fix security issues including a denial or service or the possible execution of arbitrary code if untrusted XML is processed.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-324-01 libxml2`
OID:1.3.6.1.4.1.25623.1.0.61909
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2008-4225, CVE-2008-4226`

High (CVSS: 8.5)
NVT: Slackware Advisory SSA:2008-333-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2008-333-01.

Vulnerability Detection Result
`Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-333-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, and -current to fix a possible security vulnerability involving the reading of uninitialized memory.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-333-01 samba`
OID:1.3.6.1.4.1.25623.1.0.61948
Version used: `$Revision: 6018 $`

References
`CVE: CVE-2008-4314`

High (CVSS: 8.5)
NVT: Slackware Advisory SSA:2008-333-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2008-333-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

. . . continues on next page . . .

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-333-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, and -current to fix a possible security vulnerability involving the reading of uninitialized memory.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-333-01 samba`
OID:1.3.6.1.4.1.25623.1.0.61948
Version used: `$Revision: 6018 $`

References
`CVE: CVE-2008-4314`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2009-083-01 lcms

Summary
The remote host is missing an update as announced via advisory SSA:2009-083-01.

Vulnerability Detection Result
`Package lcms-1.15-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-083-01

Vulnerability Insight
New lcms packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-083-01 lcms`
OID:1.3.6.1.4.1.25623.1.0.63697
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2009-0581, CVE-2009-0723, CVE-2009-0733`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2009-083-01 lcms

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update as announced via advisory SSA:2009-083-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-083-01

Vulnerability Insight
New lcms packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-083-01 lcms`
OID:1.3.6.1.4.1.25623.1.0.63697
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2009-0581, CVE-2009-0723, CVE-2009-0733`

High (CVSS: 7.2)
NVT: Slackware Advisory SSA:2009-111-01 udev

Summary
The remote host is missing an update as announced via advisory SSA:2009-111-01.

Vulnerability Detection Result
`Package udev-097-i486-10 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-111-01

Vulnerability Insight
New udev packages are available for Slackware 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix security issues.
The udev packages in Slackware 10.2, 11.0, 12.0, 12.1, 12.2, and -current contained a local root hole vulnerability: CVE-2009-1185
The udev packages in Slackware 12.0, 12.1, 12.2, and -current had an integer overflow which could result in a denial of service: CVE-2009-1186
Note that udev is only used with 2.6 kernels, which are not used by default with Slackware 10.2 and 11.0.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details:Slackware Advisory SSA:2009-111-01 udev
OID:1.3.6.1.4.1.25623.1.0.63895
Version used: $Revision: 5977 $

References
CVE: CVE-2009-1185, CVE-2009-1186

High (CVSS: 7.2)
NVT: Slackware Advisory SSA:2009-111-01 udev

Summary
The remote host is missing an update as announced via advisory SSA:2009-111-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-111-01

Vulnerability Insight
New udev packages are available for Slackware 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix security issues.
The udev packages in Slackware 10.2, 11.0, 12.0, 12.1, 12.2, and -current contained a local root hole vulnerability: CVE-2009-1185
The udev packages in Slackware 12.0, 12.1, 12.2, and -current had an integer overflow which could result in a denial of service: CVE-2009-1186
Note that udev is only used with 2.6 kernels, which are not used by default with Slackware 10.2 and 11.0.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2009-111-01 udev
OID:1.3.6.1.4.1.25623.1.0.63895
Version used: $Revision: 5977 $

References
CVE: CVE-2009-1185, CVE-2009-1186

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2009-129-01 xpdf

Summary
The remote host is missing an update as announced via advisory SSA:2009-129-01.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Package xpdf-3.01-i386-1 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-129-01

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2009-129-01 xpdf
OID:1.3.6.1.4.1.25623.1.0.63964
Version used: $Revision: 6022 $

References
CVE: CVE-2009-0146, CVE-2009-0147, CVE-2009-0165, CVE-2009-0166, CVE-2009-0799,
↪CVE-2009-0800, CVE-2009-1179, CVE-2009-1180, CVE-2009-1181, CVE-2009-1182, CVE
↪-2009-1183

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2009-129-01 xpdf

Summary
The remote host is missing an update as announced via advisory SSA:2009-129-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-129-01

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2009-129-01 xpdf
OID:1.3.6.1.4.1.25623.1.0.63964
Version used: $Revision: 6022 $

References
CVE: CVE-2009-0146, CVE-2009-0147, CVE-2009-0165, CVE-2009-0166, CVE-2009-0799,
↪CVE-2009-0800, CVE-2009-1179, CVE-2009-1180, CVE-2009-1181, CVE-2009-1182, CVE
↪-2009-1183

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2009-134-01 cyrus-sasl

Summary
The remote host is missing an update as announced via advisory SSA:2009-134-01.

Vulnerability Detection Result
`Package cyrus-sasl-2.1.22-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-134-01

Vulnerability Insight
New cyrus-sasl packages are available for Slackware 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue. A buffer overflow in the sasl_encode64() function could lead to a denial of service or possible execution of arbitrary code.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-134-01 cyrus-sasl`
OID:1.3.6.1.4.1.25623.1.0.63997
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2009-0688`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2009-134-01 cyrus-sasl

Summary
The remote host is missing an update as announced via advisory SSA:2009-134-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-134-01

Vulnerability Insight
New cyrus-sasl packages are available for Slackware 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue. A buffer overflow in the sasl_encode64() function could lead to a denial of service or possible execution of arbitrary code.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-134-01 cyrus-sasl`
OID:1.3.6.1.4.1.25623.1.0.63997

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: $Revision: 5999 $

References
CVE: CVE-2009-0688

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2009-177-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2009-177-01.

Vulnerability Detection Result
Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-177-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2009-177-01 samba
OID:1.3.6.1.4.1.25623.1.0.64316
Version used: $Revision: 5931 $

References
CVE: CVE-2009-1888, CVE-2009-1886

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2009-177-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2009-177-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-177-01

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-177-01 samba`
OID:1.3.6.1.4.1.25623.1.0.64316
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2009-1888, CVE-2009-1886`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2009-226-01 curl

Summary
The remote host is missing an update as announced via advisory SSA:2009-226-01.

Vulnerability Detection Result
`Package curl-7.15.5-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-226-01

Vulnerability Insight
New curl packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.
For more information, see: http://curl.haxx.se/docs/security.html

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-226-01 curl`
OID:1.3.6.1.4.1.25623.1.0.64772
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2009-2417`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2009-226-01 curl

Summary
The remote host is missing an update as announced via advisory SSA:2009-226-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-226-01

Vulnerability Insight
New curl packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.
For more information, see: http://curl.haxx.se/docs/security.html

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-226-01 curl`
OID:1.3.6.1.4.1.25623.1.0.64772
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2009-2417`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2009-302-01 xpdf

Summary
The remote host is missing an update as announced via advisory SSA:2009-302-01.

Vulnerability Detection Result
`Package xpdf-3.01-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-302-01

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-302-01 xpdf`
OID:1.3.6.1.4.1.25623.1.0.66151
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2009-3603, CVE-2009-3604, CVE-2009-3605, CVE-2009-3606, CVE-2009-3608,`
`↪CVE-2009-3609`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2009-302-01 xpdf

Summary
The remote host is missing an update as announced via advisory SSA:2009-302-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-302-01

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-302-01 xpdf`
OID:1.3.6.1.4.1.25623.1.0.66151
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2009-3603, CVE-2009-3604, CVE-2009-3605, CVE-2009-3606, CVE-2009-3608,`
`↪CVE-2009-3609`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2010-060-02 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-060-02.

Vulnerability Detection Result
`Package openssl-0.9.8d-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-060-02

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-060-02 openssl`
OID:1.3.6.1.4.1.25623.1.0.67042
Version used: `$Revision: 5956 $`

. . . continues on next page . . .

... continued from previous page ...

References
CVE: CVE-2008-1678, CVE-2009-1378, CVE-2009-1377, CVE-2009-1379, CVE-2009-3245, ↪CVE-2009-4355

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2010-060-02 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-060-02.

Vulnerability Detection Result
Package openssl-solibs-0.9.8d-i486-1 is installed which is known to be vulnerabl ↪e.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-060-02

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2010-060-02 openssl
OID:1.3.6.1.4.1.25623.1.0.67042
Version used: $Revision: 5956 $

References
CVE: CVE-2008-1678, CVE-2009-1378, CVE-2009-1377, CVE-2009-1379, CVE-2009-3245, ↪CVE-2009-4355

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2010-060-02 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-060-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-060-02

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-060-02 openssl`
OID:1.3.6.1.4.1.25623.1.0.67042
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2008-1678, CVE-2009-1378, CVE-2009-1377, CVE-2009-1379, CVE-2009-3245, ↪CVE-2009-4355`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-169-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2010-169-01.

Vulnerability Detection Result
`Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-169-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and 13.0 to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-169-01 samba`
OID:1.3.6.1.4.1.25623.1.0.67642
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2010-2063`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-169-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2010-169-01.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-169-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and 13.0 to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-169-01 samba`
OID:1.3.6.1.4.1.25623.1.0.67642
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2010-2063`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-180-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2010-180-01.

Vulnerability Detection Result
`Package libpng-1.2.12-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-180-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-180-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.68165
Version used: `$Revision: 5963 $`

References
`CVE: CVE-2010-1205, CVE-2010-2249`

... continues on next page ...

... continued from previous page ...

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-180-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2010-180-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-180-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-180-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.68165
Version used: `$Revision: 5963 $`

References
`CVE: CVE-2010-1205, CVE-2010-2249`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-257-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2010-257-01.

Vulnerability Detection Result
`Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-257-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-257-01 samba`
OID:1.3.6.1.4.1.25623.1.0.68180

... continues on next page ...

. . . continued from previous page . . .

Version used: `$Revision: 6022 $`

References
`CVE: CVE-2010-3069`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-257-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2010-257-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-257-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-257-01 samba`
OID:1.3.6.1.4.1.25623.1.0.68180
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2010-3069`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-258-03 sudo redo

Summary
The remote host is missing an update as announced via advisory SSA:2010-258-03.

Vulnerability Detection Result
`Package sudo-1.6.8-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-258-03

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

New sudo packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a directory permissions issue. These replacement packages restore the correct permissions to /var.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-258-03 sudo redo`
OID:1.3.6.1.4.1.25623.1.0.68178
Version used: `$Revision: 5950 $`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-258-03 sudo redo

Summary
The remote host is missing an update as announced via advisory SSA:2010-258-03.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-258-03

Vulnerability Insight
New sudo packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a directory permissions issue. These replacement packages restore the correct permissions to /var.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-258-03 sudo redo`
OID:1.3.6.1.4.1.25623.1.0.68178
Version used: `$Revision: 5950 $`

High (CVSS: 7.1)
NVT: Slackware Advisory SSA:2010-305-03 proftpd

Summary
The remote host is missing an update as announced via advisory SSA:2010-305-03.

Vulnerability Detection Result
`Package proftpd-1.3.0a-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-305-03

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
New proftpd packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to a fix security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-305-03 proftpd`
OID:1.3.6.1.4.1.25623.1.0.68466
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2010-3867`

High (CVSS: 7.1)
NVT: Slackware Advisory SSA:2010-305-03 proftpd

Summary
The remote host is missing an update as announced via advisory SSA:2010-305-03.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-305-03

Vulnerability Insight
New proftpd packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to a fix security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-305-03 proftpd`
OID:1.3.6.1.4.1.25623.1.0.68466
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2010-3867`

High (CVSS: 7.6)
NVT: Slackware Advisory SSA:2010-326-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-326-01.

Vulnerability Detection Result
`Package openssl-0.9.8d-i486-1 is installed which is known to be vulnerable.`

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-326-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-326-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.68673
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2010-2939, CVE-2010-3864`

High (CVSS: 7.6)
NVT: Slackware Advisory SSA:2010-326-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-326-01.

Vulnerability Detection Result
`Package openssl-solibs-0.9.8d-i486-1 is installed which is known to be vulnerabl`
`↪e.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-326-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-326-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.68673
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2010-2939, CVE-2010-3864`

... continues on next page ...

... continued from previous page ...

High (CVSS: 7.6)
NVT: Slackware Advisory SSA:2010-326-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-326-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-326-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-326-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.68673
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2010-2939, CVE-2010-3864`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-340-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-340-01.

Vulnerability Detection Result
`Package openssl-0.9.8d-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-340-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-340-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.68671

... continues on next page ...

... continued from previous page ...

Version used: `$Revision: 5931 $`

References
`CVE: CVE-2010-4180, CVE-2010-4252`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-340-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-340-01.

Vulnerability Detection Result
`Package openssl-solibs-0.9.8d-i486-1 is installed which is known to be vulnerabl`
`↪e.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-340-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-340-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.68671
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2010-4180, CVE-2010-4252`

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2010-340-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-340-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-340-01

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-340-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.68671
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2010-4180, CVE-2010-4252`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2011-098-01 libtiff

Summary
The remote host is missing an update as announced via advisory SSA:2011-098-01.

Vulnerability Detection Result
`Package libtiff-3.8.2-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-098-01

Vulnerability Insight
New libtiff packages are available for Slackware 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-098-01 libtiff`
OID:1.3.6.1.4.1.25623.1.0.69579
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2011-0192, CVE-2011-1167`

High (CVSS: 9.3)
NVT: Slackware Advisory SSA:2011-098-01 libtiff

Summary
The remote host is missing an update as announced via advisory SSA:2011-098-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-098-01

Vulnerability Insight
New libtiff packages are available for Slackware 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-098-01 libtiff`
OID:1.3.6.1.4.1.25623.1.0.69579
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2011-0192, CVE-2011-1167`

High (CVSS: 9.0)
NVT: Slackware Advisory SSA:2012-041-04 proftpd

Summary
The remote host is missing an update as announced via advisory SSA:2012-041-04.

Vulnerability Detection Result
`Package proftpd-1.3.0a-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-041-04

Vulnerability Insight
New proftpd packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2012-041-04 proftpd`
OID:1.3.6.1.4.1.25623.1.0.71967
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2011-4130`

High (CVSS: 9.0)
NVT: Slackware Advisory SSA:2012-041-04 proftpd

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update as announced via advisory SSA:2012-041-04.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-041-04

Vulnerability Insight
New proftpd packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2012-041-04 proftpd`
OID:1.3.6.1.4.1.25623.1.0.71967
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2011-4130`

High (CVSS: 8.5)
NVT: Slackware Advisory SSA:2012-166-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2012-166-01.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-166-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2012-166-01 bind`
OID:1.3.6.1.4.1.25623.1.0.71984
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2012-1033, CVE-2012-1667`

High (CVSS: 8.5)
NVT: Slackware Advisory SSA:2012-166-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2012-166-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-166-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2012-166-01 bind`
OID:1.3.6.1.4.1.25623.1.0.71984
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2012-1033, CVE-2012-1667`

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2012-176-01 freetype

Summary
The remote host is missing an update as announced via advisory SSA:2012-176-01.

Vulnerability Detection Result
`Package freetype-1.3.1-i386-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-176-01

Vulnerability Insight
New freetype packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2012-176-01 freetype`
OID:1.3.6.1.4.1.25623.1.0.71978
Version used: `$Revision: 5931 $`

. . . continues on next page . . .

... continued from previous page ...

References
CVE: CVE-2012-1126, CVE-2012-1144

High (CVSS: 10.0)
NVT: Slackware Advisory SSA:2012-176-01 freetype

Summary
The remote host is missing an update as announced via advisory SSA:2012-176-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-176-01

Vulnerability Insight
New freetype packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2012-176-01 freetype
OID:1.3.6.1.4.1.25623.1.0.71978
Version used: $Revision: 5931 $

References
CVE: CVE-2012-1126, CVE-2012-1144

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2012-200-01 libexif

Summary
The remote host is missing an update as announced via advisory SSA:2012-200-01.

Vulnerability Detection Result
Package libexif-0.6.13-i486-2 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-200-01

Vulnerability Insight
New libexif packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:Slackware Advisory SSA:2012-200-01 libexif
OID:1.3.6.1.4.1.25623.1.0.71972
Version used: $Revision: 6022 $

References
CVE: CVE-2012-2812, CVE-2012-2813, CVE-2012-2814, CVE-2012-2836, CVE-2012-2837,
↪CVE-2012-2840, CVE-2012-2841, CVE-2012-2845

High (CVSS: 7.5)
NVT: Slackware Advisory SSA:2012-200-01 libexif

Summary
The remote host is missing an update as announced via advisory SSA:2012-200-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-200-01

Vulnerability Insight
New libexif packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2012-200-01 libexif
OID:1.3.6.1.4.1.25623.1.0.71972
Version used: $Revision: 6022 $

References
CVE: CVE-2012-2812, CVE-2012-2813, CVE-2012-2814, CVE-2012-2836, CVE-2012-2837,
↪CVE-2012-2840, CVE-2012-2841, CVE-2012-2845

High (CVSS: 8.5)
NVT: Subversion Binary Delta Processing Multiple Integer Overflow Vulnerabilities

Product detection result
cpe:/a:subversion:subversion:1
Detected by Subversion Version Detection (OID: 1.3.6.1.4.1.25623.1.0.101103)

Summary
The host is installed with Subversion and is prone to multiple Integer Overflow Vulnerabilities.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version:
Fixed version: 1.5.7/1.6.4

Impact
Attackers can exploit these issues to compromise an application using the library or crash the application, resulting into a denial of service conditions.
Impact Level: Application

Solution
Solution type: VendorFix
Apply the patch or Upgrade to Subversion version 1.5.7 or 1.6.4 http://subversion.tigris.org/security/CVE-2009-2411-advisory.txt http://subversion.tigris.org/project_packages.html
**** NOTE: Please ignore this warning if the patch is applied. *****

Affected Software/OS
Subversion version 1.5.6 and prior Subversion version 1.6.0 through 1.6.3

Vulnerability Insight
The flaws are due to input validation errors in the processing of svndiff streams in the 'libsvn_delta' library.

Vulnerability Detection Method
Details:Subversion Binary Delta Processing Multiple Integer Overflow Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.101104
Version used: $Revision: 5122 $

Product Detection Result
Product: cpe:/a:subversion:subversion:1
Method: Subversion Version Detection
OID: 1.3.6.1.4.1.25623.1.0.101103)

References
CVE: CVE-2009-2411
BID:35983
Other:
URL:http://secunia.com/advisories/36184/
URL:http://securitytracker.com/alerts/2009/Aug/1022697.html
URL:http://subversion.tigris.org/security/CVE-2009-2411-advisory.txt

High (CVSS: 10.0)
NVT: Sun Java JDK/JRE Multiple Vulnerabilities - Aug09

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with Sun Java JDK/JRE and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allows remote attacker to gain privileges via untrusted applet or Java Web Start application in the context of the affected system. Impact Level: System/Application

Solution
Upgrade to JDK/JRE version 6 Update 15 or 5 Update 20 http://java.sun.com/javase/downloads/index.jsp http://java.sun.com/javase/downloads/index_jdk5.jsp or Apply the patch from below link, http://sunsolve.sun.com/search/document.do?assetkey=1-21-125136-16-1 http://sunsolve.sun.com/search/document.do?assetkey=1-21-125139-16-1 http://sunsolve.sun.com/search/document.do?assetkey=1-21-118667-22-1
*** NOTE: Ignore this warning if above mentioned patch is already applied. *****

Affected Software/OS
Sun Java JDK/JRE version 6 before Update 15 or 5.0 before Update 20

Vulnerability Insight
Refer to the reference links for more information on the vulnerabilities.

Vulnerability Detection Method
Details:Sun Java JDK/JRE Multiple Vulnerabilities - Aug09
OID:1.3.6.1.4.1.25623.1.0.800867
Version used: $Revision: 4869 $

References
CVE: CVE-2009-2670, CVE-2009-2671, CVE-2009-2672, CVE-2009-2673, CVE-2009-2675, ↪CVE-2009-2475, CVE-2009-2689
BID:35939, 35943, 35944
Other:
URL:http://secunia.com/advisories/36159
URL:http://secunia.com/advisories/36162
URL:http://secunia.com/advisories/36180
URL:http://secunia.com/advisories/36199
URL:http://java.sun.com/javase/6/webnotes/6u15.html
URL:http://java.sun.com/j2se/1.5.0/ReleaseNotes.html
URL:http://sunsolve.sun.com/search/document.do?assetkey=1-66-263408-1
URL:http://sunsolve.sun.com/search/document.do?assetkey=1-66-263409-1
URL:http://sunsolve.sun.com/search/document.do?assetkey=1-66-263488-1

High (CVSS: 9.3)
NVT: Sun Java JDK/JRE Multiple Vulnerabilities - Nov09 (Linux)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Sun Java JDK/JRE and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows remote attacker to execute arbitrary code, gain escalated privileges, bypass security restrictions and cause denial of service attacks inside the context of the affected system. Impact Level: System/Application.

Solution
Solution type: VendorFix
Upgrade to JDK/JRE version 6 Update 17 or later, http://java.sun.com/javase/downloads/index.jsp OR Upgrade to JDK/JRE version 5 Update 22 http://java.sun.com/javase/downloads/index_jdk5.jsp OR Upgrade to JDK/JRE version 1.4.2_24 http://java.sun.com/j2se/1.4.2/download.html OR Upgrade to JDK/JRE version 1.3.1_27 http://java.sun.com/j2se/1.3/download.html

Affected Software/OS
Sun Java JDK/JRE 6 prior to 6 Update 17 Sun Java JDK/JRE 5 prior to 5 Update 22 Sun Java JDK/JRE 1.4.x prior to 1.4.2_24 Sun Java JDK/JRE 1.3.x prior to 1.3.1_27 on Linux.

Vulnerability Insight
Multiple flaws occur due to, - Error when decoding 'DER' encoded data and parsing HTTP headers. - Error when verifying 'HMAC' digests. - Integer overflow error in the 'JPEG JFIF' Decoder while processing malicious image files. - A buffer overflow error in the 'setDiffICM()' and 'setBytePixels()' functions in the Abstract Window Toolkit (AWT). - Unspecified error due to improper parsing of color profiles of images. - A buffer overflow error due to improper implementation of the 'HsbParser.getSoundBank()' function. - Three unspecified errors when processing audio or image files.

Vulnerability Detection Method
Details:`Sun Java JDK/JRE Multiple Vulnerabilities - Nov09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800975
Version used: `$Revision: 4869 $`

References
```
CVE: CVE-2009-3877, CVE-2009-3876, CVE-2009-3875, CVE-2009-3873, CVE-2009-3874,
↪CVE-2009-3872, CVE-2009-3871, CVE-2009-3869, CVE-2009-3868, CVE-2009-3867
BID:36881
Other:
  URL:http://secunia.com/advisories/37231
   URL:http://java.sun.com/javase/6/webnotes/6u17.html
   URL:http://www.vupen.com/english/advisories/2009/3131
```

High (CVSS: 10.0)
NVT: Sun Java JRE Multiple Vulnerabilities (Linux)

Summary
This host is installed with Sun Java JRE and is prone to Multiple Vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows remote attacker to cause XSS, arbitrary code execution, various buffer overflows, bypass security restrictions and can cause denial of service attacks inside the context of the affected system. Impact Level: System

Solution
Solution type: VendorFix
Upgrade to JDK/JRE version 6 Update 13 http://java.sun.com/javase/downloads/index.jsp OR Upgrade to JDK/JRE version 5 Update 18 http://java.sun.com/javase/downloads/index_jdk5.jsp OR Upgrade to SDK/JRE version 1.4.2_20 http://java.sun.com/j2se/1.4.2/download.html OR Upgrade to SDK/JRE version 1.3.1_25 http://java.sun.com/j2se/1.3/download.html

Affected Software/OS
Sun Java JRE 6 Update 12 and prior. Sun Java JRE 5.0 Update 17 and prior. Sun Java JRE 1.4.2_19 and prior. Sun Java JRE 1.3.1_24 and prior.

Vulnerability Insight
For more information about vulnerabilities on Sun Java go through reference.

Vulnerability Detection Method
Details:Sun Java JRE Multiple Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.800386
Version used: $Revision: 4869 $

References
```
CVE: CVE-2009-1093, CVE-2009-1094, CVE-2009-1095, CVE-2009-1096, CVE-2009-1097,
↪CVE-2009-1098, CVE-2009-1099, CVE-2009-1100, CVE-2009-1101, CVE-2009-1102, CVE
↪-2009-1103, CVE-2009-1104, CVE-2009-1105, CVE-2009-1106, CVE-2009-1107
BID:34240
Other:
  URL:http://secunia.com/advisories/34489
   URL:http://rhn.redhat.com/errata/RHSA-2009-0394.html
   URL:http://sunsolve.sun.com/search/document.do?assetkey=1-66-254569-1
   URL:http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00001.htm
↪l
```

... continues on next page ...

... continued from previous page ...

High (CVSS: 10.0)
NVT: Sun Java SE Multiple Unspecified Vulnerabilities

Summary
This host is installed with Sun Java SE and is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Impact is unknow. Impact Level: System/Application

Solution
Upgrade to Java SE version 5 Update 20 http://java.sun.com/javase/downloads/index_jdk5.jsp or Apply the patch from below link, http://sunsolve.sun.com/search/document.do?assetkey=1-21-118667-22-1
*** NOTE: Ignore this warning if above mentioned patch is already applied. *****

Affected Software/OS
Sun Java SE version 5.0 before Update 20

Vulnerability Insight
Refer to the SunSolve bugId 6406003/6429594/6444262 for more information.

Vulnerability Detection Method
Details:`Sun Java SE Multiple Unspecified Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.900819
Version used: `$Revision: 5122 $`

References
`CVE: CVE-2009-2721, CVE-2009-2722, CVE-2009-2723, CVE-2009-2724`
`Other:`
`URL:http://java.sun.com/j2se/1.5.0/ReleaseNotes.html`

High (CVSS: 9.3)
NVT: TOR Privilege Escalation Vulnerability (Linux)

Summary
This host is installed with TOR and is prone to Privilege Escalation vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will let the attacker gain privileges and escalate the privileges in malicious ways.

Solution
Solution type: VendorFix
Upgrade to the latest version 0.2.0.32 http://www.torproject.org/download.html.en

Affected Software/OS
Tor version 0.2.0.31 or prior.

Vulnerability Insight
The flaws are due to, - an application does not properly drop privileges to the primary groups of the user specified by the User Parameter. - a ClientDNSRejectInternalAddresses configuration option is not always enforced which weaknesses the application security.

Vulnerability Detection Method
Details:`TOR Privilege Escalation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900424
Version used: `$Revision: 4557 $`

References
`CVE: CVE-2008-5397, CVE-2008-5398`
`BID:32648`
`Other:`
`URL:http://www.torproject.org`
`URL:http://secunia.com/advisories/33025`

High (CVSS: 10.0)
NVT: Tor Unspecified Heap Based Buffer Overflow Vulnerability (Linux)

Summary
This host is installed with Tor and is prone to heap based buffer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code in the context of the user running the application. Failed exploit attempts will likely result in denial-of-service conditions.
Impact level: Application

Solution
Solution type: VendorFix
Upgrade to version 0.2.1.28 or 0.2.2.20-alpha or later http://www.torproject.org/download/download.html.en

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Tor version prior to 0.2.1.28 and 0.2.2.x before 0.2.2.20-alpha on Linux.

Vulnerability Insight
The issue is caused by an unknown heap overflow error when processing user-supplied data, which can be exploited to cause a heap-based buffer overflow.

Vulnerability Detection Method
Details:`Tor Unspecified Heap Based Buffer Overflow Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.902332
Version used: `$Revision: 3114 $`

References
`CVE: CVE-2010-1676`
`BID:45500`
`Other:`
`URL:http://secunia.com/advisories/42536`
`URL:http://www.vupen.com/english/advisories/2010/3290`

High (CVSS: 10.0)
NVT: Tor Unspecified Remote Memory Corruption Vulnerability (Linux)

Summary
This host is installed with Tor and is prone to unspecified remote Memory Corruption vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
A remote attcker can execute arbitrary code on the target system and can cause denial-of-service.
Impact level: Application

Solution
Solution type: VendorFix
Upgrade to version 0.2.0.33 or later https://www.torproject.org/download-unix.html.en

Affected Software/OS
Tor version prior to 0.2.0.33 on Linux.

Vulnerability Insight
Due to unknown impact, remote attachers can trigger heap corruption on the application.

Vulnerability Detection Method
Details:`Tor Unspecified Remote Memory Corruption Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800350

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 4892 $

References
CVE: CVE-2009-0414
BID:33399
Other:
URL:http://secunia.com/advisories/33635
URL:http://secunia.com/advisories/33677
URL:http://securitytracker.com/alerts/2009/Jan/1021633.html
URL:http://blog.torproject.org/blog/tor-0.2.0.33-stable-released

High (CVSS: 9.3)
NVT: VLC Media Player '.mkv' Code Execution Vulnerability (Linux)

Summary
The host is installed with VLC Media Player and is prone to arbitrary code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attackers to execute arbitrary code by tricking a user into opening a specially crafted MKV file. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to the VLC media player version 1.1.7 or later, For updates refer to http://download.videolan.org/pub/videolan/vlc/

Affected Software/OS
VLC media player version 1.1.6.1 and prior on Linux

Vulnerability Insight
The flaw is due to an input validation error within the 'MKV_IS_ID' macro in 'modules/demux/mkv/mkv.hpp' of the MKV demuxer, when parsing the MKV file.

Vulnerability Detection Method
Details:VLC Media Player '.mkv' Code Execution Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.902339
Version used: $Revision: 3570 $

References
CVE: CVE-2011-0531
BID:46060
Other:

... continues on next page ...

... continued from previous page ...

URL:http://xforce.iss.net/xforce/xfdb/65045
URL:http://www.securitytracker.com/id?1025018

High (CVSS: 9.3)
NVT: VLC Media Player 'CDG decoder' multiple buffer overflow vulnerabilities (Linux)

Summary
The host is installed with VLC Media Player and is prone multiple buffer overflow vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attackers to crash the affected application, or execute arbitrary code by convincing a user to open a malicious CD+G (CD+Graphics) media file or visit a specially crafted web page. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to the VLC media player version 1.1.6 or later, For updates refer to http://download.videolan.org/pub/videolan/vlc/

Affected Software/OS
VLC media player version prior to 1.1.6 on Linux

Vulnerability Insight
The flaws are due to an array indexing errors in the 'DecodeTileBlock()' and 'DecodeScroll()' [modules/codec/cdg.c] functions within the CDG decoder module when processing malformed data.

Vulnerability Detection Method
Details:VLC Media Player 'CDG decoder' multiple buffer overflow vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.801727
Version used: $Revision: 3117 $

References
CVE: CVE-2011-0021
Other:
URL:http://www.vupen.com/english/advisories/2011/0185
URL:http://openwall.com/lists/oss-security/2011/01/20/3

High (CVSS: 7.5)
NVT: VLC Media Player 'real_get_rdt_chunk' BOF Vulnerability-02 Jan15 (Linux)

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:videolan:vlc_media_player:0.8.4a:a
Detected by VLC Media Player Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1
↪.0.900529)

Summary
The host is installed with VLC media player and is prone to buffer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attacker to execute an arbitrary code within the context of the VLC media player and potentially compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to VideoLAN VLC media player version 1.0.1 or later. For updates refer http://www.videolan.org/

Affected Software/OS
VideoLAN VLC media player before 1.0.1 on Linux.

Vulnerability Insight
The error exists due to an integer underflow in the 'real_get_rdt_chunk' function within modules/access/rtsp/real.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:VLC Media Player 'real_get_rdt_chunk' BOF Vulnerability-02 Jan15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805312
Version used: $Revision: 3006 $

Product Detection Result
Product: cpe:/a:videolan:vlc_media_player:0.8.4a:a
Method: VLC Media Player Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.900529)

References
CVE: CVE-2010-2062
Other:
URL:http://secunia.com/advisories/36037/
URL:http://seclists.org/fulldisclosure/2009/Jul/418
URL:http://packetstormsecurity.com/files/cve/CVE-2010-2062

High (CVSS: 7.5)
NVT: VLC Media Player M3U Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:videolan:vlc_media_player:0.8.4a:a
Detected by VLC Media Player Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1
↪.0.900529)

Summary
This host is installed with VLC Media Player and is prone to denial of service and remote code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to cause denial of service and possibly execute arbitrary remote code.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to VLC media player version 2.1.0 or later, For updates refer to http://www.videolan.org/vlc

Affected Software/OS
VLC media player version 2.0.8 and prior on Linux

Vulnerability Insight
The flaw exist due to improper handling of a specially crafted M3U file.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:VLC Media Player M3U Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.804127
Version used: $Revision: 3561 $

Product Detection Result
Product: cpe:/a:videolan:vlc_media_player:0.8.4a:a
Method: VLC Media Player Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.900529)

References
CVE: CVE-2013-6283
BID:61844
Other:

. . . continues on next page . . .

... continued from previous page ...

URL:http://en.securitylab.ru/nvd/447008.php
URL:http://www.exploit-db.com/exploits/27700

High (CVSS: 7.5)
NVT: VLC Media Player Multiple Buffer Overflow Vulnerabilities-01 Jan15 (Linux)

Product detection result
cpe:/a:videolan:vlc_media_player:0.8.4a:a
Detected by VLC Media Player Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1
↪.0.900529)

Summary
The host is installed with VLC media player and is prone to multiple buffer overflow vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to conduct a denial of service attack or potentially the execution of arbitrary code.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to VideoLAN VLC media player version 1.0.2 or later. For updates refer http://www.videolan.org/

Affected Software/OS
VideoLAN VLC media player before 1.0.2 on Linux.

Vulnerability Insight
Multiple flaws are due to overflow conditions in the, - ASF_ObjectDumpDebug function within modules/demux/asf/libasf.c script, - AVI_ChunkDumpDebug_level function within modules/demux/avi/libavi.c script, - AVI_ChunkDumpDebug_level function within modules/demux/avi/libavi.c script - MP4_BoxDumpStructure function within modules/demux/mp4/libmp4.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:VLC Media Player Multiple Buffer Overflow Vulnerabilities-01 Jan15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805309
Version used: $Revision: 3499 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:videolan:vlc_media_player:0.8.4a:a
Method: VLC Media Player Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.900529)

References
CVE: CVE-2011-3623
Other:
URL:http://www.videolan.org/security/sa0901.html
URL:http://packetstormsecurity.com/files/cve/CVE-2011-3623

High (CVSS: 9.3)
NVT: VLC Media Player Multiple Stack-Based BOF Vulnerabilities - Nov08 (Linux)

Summary
This host is installed with VLC Media Player and is prone to Multiple Stack-Based Buffer Overflow Vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows attackers to execute arbitrary code within the context of the VLC media player by tricking a user into opening a specially crafted file or can even crash an affected application. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to 0.9.6, or Apply the available patch from below link,
http://git.videolan.org/?p=vlc.git a=commitdiff h=e3cef651125701a2e33a8d75b815b3e39681a447
http://git.videolan.org/?p=vlc.git a=commitdiff h=5f63f1562d43f32331006c2c1a61742de031b84d
*** NOTE: Ignore this warning if above mentioned patch is already applied. *****

Affected Software/OS
VLC media player 0.5.0 through 0.9.5 on Windows (Any).

Vulnerability Insight
The flaws are caused while parsing, - header of an invalid CUE image file related to modules/access/vcd/cdrom.c. - an invalid RealText(rt) subtitle file related to the ParseRealText function in modules/demux/subtitle.c.

Vulnerability Detection Method
Details:VLC Media Player Multiple Stack-Based BOF Vulnerabilities - Nov08 (Linux)
OID:1.3.6.1.4.1.25623.1.0.800133
Version used: $Revision: 5158 $

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2008-5032, CVE-2008-5036
BID:32125
Other:
URL:http://www.videolan.org/security/sa0810.html
URL:http://www.trapkit.de/advisories/TKADV2008-011.txt
URL:http://www.trapkit.de/advisories/TKADV2008-012.txt

High (CVSS: 9.3)
NVT: VLC Media Player Multiple Vulnerabilities - Mar 12 (Linux)

Summary
This host is installed with VLC Media Player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attackers to cause a denial of service or possibly execute arbitrary code via crafted streams. Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to VLC media player version 2.0.1 or later For updates refer to http://www.videolan.org/vlc/

Affected Software/OS
VLC media player version prior to 2.0.1 on Linux

Vulnerability Insight
The flaws are due to multiple buffer overflow errors in the application, which allows remote attackers to execute arbitrary code via crafted MMS:// stream and Real RTSP streams.

Vulnerability Detection Method
Details:VLC Media Player Multiple Vulnerabilities - Mar 12 (Linux)
OID:1.3.6.1.4.1.25623.1.0.802723
Version used: $Revision: 5956 $

References
CVE: CVE-2012-1775, CVE-2012-1776
Other:
URL:http://www.videolan.org/security/sa1201.html
URL:http://www.videolan.org/security/sa1202.html

High (CVSS: 7.5)
NVT: VLC Media Player Multiple Vulnerabilities-03 Jan15 (Linux)

Product detection result
cpe:/a:videolan:vlc_media_player:0.8.4a:a
Detected by VLC Media Player Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1
↪.0.900529)

Summary
The host is installed with VLC media player and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to conduct a denial of service or potentially compromise a user's system.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to VideoLAN VLC media player version 1.0.6 or later. For updates refer http://www.videolan.org/

Affected Software/OS
VideoLAN VLC media player before 1.0.6 on Linux.

Vulnerability Insight
Multiple flaws are due to, - Multiple errors in the A/52 audio decoder, DTS audio decoder, MPEG audio decoder, AVI demuxer, ASF demuxer and Matroska demuxer. - An error when processing XSPF playlists. - A use-after-free error when attempting to create a playlist of the contents of a malformed zip archive. - An error in the RTMP implementation.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:VLC Media Player Multiple Vulnerabilities-03 Jan15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805314
Version used: $Revision: 3499 $

Product Detection Result
Product: cpe:/a:videolan:vlc_media_player:0.8.4a:a
Method: VLC Media Player Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.900529)

References
CVE: CVE-2010-1445, CVE-2010-1444, CVE-2010-1443, CVE-2010-1442, CVE-2010-1441

. . . continues on next page . . .

... continued from previous page ...

Other:
URL:http://secunia.com/advisories/39558
URL:http://www.videolan.org/security/sa1003.html

High (CVSS: 10.0)
NVT: Xpdf Multiple Vulnerabilities

Product detection result
cpe:/a:foolabs:xpdf:3.01
Detected by Xpdf Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900466)

Summary
The PDF viewer Xpdf is prone to multiple vulnerabilities on Linux systems that can lead to arbitrary code execution.

Vulnerability Detection Result
Installed version: 3.01
Fixed version: 3.02 pl3

Impact
Successful exploitation will let the attacker craft a malicious PDF File and execute arbitrary codes into the context of the affected application to cause denial of service attacks, buffer overflow attacks, remote code executions etc.

Solution
Solution type: VendorFix
Apply Xpdf v3.02 pl3 patch: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.02pl3.patch

Affected Software/OS
Xpdf version 3.02 and prior on Linux.

Vulnerability Insight
- Integer overflow in Xpdf JBIG2 Decoder which allows the attacker create a malicious crafted PDF File and causes code execution.
- Flaws in Xpdf JBIG2 Decoder which causes buffer overflow, freeing of arbitrary memory causing Xpdf application to crash.

Vulnerability Detection Method
This test uses the xpdf detection results and checks version of each binary found on the target system. Version 3.02 and prior will raise a security alert.
Details:Xpdf Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.900457
Version used: $Revision: 5148 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:foolabs:xpdf:3.01
Method: Xpdf Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900466)

References

CVE: CVE-2009-0195, CVE-2009-0166, CVE-2009-0147, CVE-2009-0146, CVE-2009-1183,
↪CVE-2009-1182, CVE-2009-1181, CVE-2009-1179, CVE-2009-0800, CVE-2009-1180, CVE
↪-2009-0799, CVE-2009-0165
BID:34568, 34791
Other:
URL:http://secunia.com/advisories/34755
URL:https://bugzilla.redhat.com/show_bug.cgi?id=495896
URL:http://www.redhat.com/support/errata/RHSA-2009-0430.html

[return to 192.168.27.45]

2.1.2 High 22/tcp

High (CVSS: 7.5)
NVT: OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability

Summary
OpenSSH is prone to a remote memory-corruption vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker can exploit this issue to execute arbitrary code in context of the application. Failed exploits may result in denial-of- service conditions.

Solution
Updates are available.

Affected Software/OS
OpenSSH 6.4 and prior with J-PAKE implemented are vulnerable.

Vulnerability Insight
The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.

Vulnerability Detection Method
Check the version.

... continues on next page ...

... continued from previous page ...

Details:OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105001
Version used: $Revision: 4336 $

References
CVE: CVE-2014-1692
BID:65230
Other:
URL:http://www.securityfocus.com/bid/65230
URL:http://www.openssh.com

High (CVSS: 7.8)
NVT: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)

Product detection result
cpe:/a:openbsd:openssh:4.4
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is installed with openssh and is prone to denial of service and user enumeration vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4
Fixed version: 7.3

Impact
Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.3 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions before 7.3 on Linux

Vulnerability Insight
Multiple flaws exists due to, - The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication. - The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.809154
Version used: $Revision: 5352 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.4
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2016-6515, CVE-2016-6210
BID:92212
Other:
URL:http://www.openssh.com/txt/release-7.3
URL:http://seclists.org/fulldisclosure/2016/Jul/51
URL:https://security-tracker.debian.org/tracker/CVE-2016-6210
URL:http://openwall.com/lists/oss-security/2016/08/01/2

High (CVSS: 8.5)
NVT: OpenSSH Multiple Vulnerabilities

Product detection result
cpe:/a:openbsd:openssh:4.4
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is running OpenSSH and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4
Fixed version: 7.0

Impact
Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH 7.0 or later. For updates refer to http://www.openssh.com

Affected Software/OS

... continues on next page ...

... continued from previous page ...

OpenSSH versions before 7.0

Vulnerability Insight
Multiple flaws are due to: - Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd. - Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd. - vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.806052
Version used: `$Revision: 4336 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.4`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2015-6564, CVE-2015-6563, CVE-2015-5600`
`Other:`
`URL:http://seclists.org/fulldisclosure/2015/Aug/54`
`URL:http://openwall.com/lists/oss-security/2015/07/23/4`

High (CVSS: 7.5)
NVT: OpenSSH Multiple Vulnerabilities Jan17 (Linux)

Product detection result
`cpe:/a:openbsd:openssh:4.4`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4`
`Fixed version: 7.4`

Impact
Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, and allows remote attackers to execute arbitrary local PKCS#11 modules.
Impact Level: Application

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to OpenSSH version 7.4 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions before 7.4 on Linux

Vulnerability Insight
Multiple flaws exists due to, - An 'authfile.c' script does not properly consider the effects of realloc on buffer contents. - The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers. - The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used. - An untrusted search path vulnerability in ssh-agent.c in ssh-agent.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH Multiple Vulnerabilities Jan17 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.8103256
Version used: `$Revision: 5084 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.4`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012
BID:94968, 94972, 94977, 94975
Other:
  URL:https://www.openssh.com/txt/release-7.4
   URL:http://www.openwall.com/lists/oss-security/2016/12/19/2
```

High (CVSS: 7.2)
NVT: OpenSSH Privilege Escalation Vulnerability - May16

Product detection result
```
cpe:/a:openbsd:openssh:4.4
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
```

Summary
This host is installed with openssh and is prone to privilege escalation vulnerability.

Vulnerability Detection Result
```
Installed version: 4.4
Fixed version:     7.2p2-3
```

... continues on next page ...

... continued from previous page ...

Impact
Successfully exploiting this issue will allow local users to gain privileges.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.2p2-3 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions through 7.2p2

Vulnerability Insight
The flaw exists due to an error in 'do_setup_env function' in 'session.c' script in sshd which trigger a crafted environment for the /bin/login program when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH Privilege Escalation Vulnerability - May16`
OID:1.3.6.1.4.1.25623.1.0.807574
Version used: `$Revision: 5527 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.4`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2015-8325`
`Other:`
`URL:https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html`
`URL:https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4`
`↪e10a65c91810f88755`

High (CVSS: 7.5)
NVT: OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)

Product detection result
`cpe:/a:openbsd:openssh:4.4`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to security bypass vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 4.4
Fixed version: 7.2

Impact
Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.2 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions before 7.2 on Linux.

Vulnerability Insight
An access flaw was discovered in OpenSSH, It did not correctly handle failures to generate authentication cookies for untrusted X11 forwarding. A malicious or compromised remote X application could possibly use this flaw to establish a trusted connection to the local X server, even if only untrusted X11 forwarding was requested.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.810769
Version used: $Revision: 6002 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.4
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2016-1908
BID:84427
Other:
URL:http://openwall.com/lists/oss-security/2016/01/15/13
URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4
URL:http://www.openssh.com/txt/release-7.2
URL:https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6f
↪a0db113c71e234416c
URL:https://bugzilla.redhat.com/show_bug.cgi?id=1298741

High (CVSS: 9.0)
NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.
As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result
`It was possible to login with the following credentials <User>:<Password>`
`root:toor`

Solution
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Try to login with a number of known default credentials via the SSH protocol.
Details:`SSH Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: `$Revision: 5467 $`

[return to 192.168.27.45]

2.1.3 High 80/tcp

High (CVSS: 7.5)
NVT: Ajax File and Image Manager 'data.php' PHP Code Injection Vulnerability

Summary
Ajax File and Image Manager is prone to a remote PHP code-injection vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker can exploit this issue to inject and execute arbitrary PHP code in the context of the affected application. This may facilitate a compromise of the application and the underlying system other attacks are also possible.

Affected Software/OS
Ajax File and Image Manager 1.0 is vulnerable other versions may also be affected.

Vulnerability Detection Method
Details:`Ajax File and Image Manager 'data.php' PHP Code Injection Vulnerability`

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.103334
Version used: $Revision: 5747 $

References
CVE: CVE-2011-4825
BID:50523
Other:
URL:http://www.securityfocus.com/bid/50523
URL:http://www.phpletter.com/

High (CVSS: 7.1)
NVT: Apache 'mod_deflate' Denial Of Service Vulnerability - July09

Summary
This host is running Apache HTTP Server and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause Denial of Service to the legitimate user by CPU consumption. Impact Level: Application

Solution
Fixed in the SVN repository. http://svn.apache.org/viewvc?view=rev&revision=791454
**** NOTE: Ignore this warning if above mentioned patch is already applied. ******

Affected Software/OS
Apache HTTP Server version 2.2.11 and prior

Vulnerability Insight
The flaw is due to error in 'mod_deflate' module which can cause a high CPU load by requesting large files which are compressed and then disconnecting.

Vulnerability Detection Method
Details:Apache 'mod_deflate' Denial Of Service Vulnerability - July09
OID:1.3.6.1.4.1.25623.1.0.800837
Version used: $Revision: 4865 $

References
CVE: CVE-2009-1891
BID:35623
Other:
URL:http://secunia.com/advisories/35781
URL:http://www.vupen.com/english/advisories/2009/1841
URL:https://rhn.redhat.com/errata/RHSA-2009-1148.html
URL:https://bugzilla.redhat.com/show_bug.cgi?id=509125

High (CVSS: 7.5)
NVT: Apache 'mod_proxy_ftp' Module Command Injection Vulnerability (Linux)

Summary
The host is running Apache and is prone to Command Injection vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attackers to bypass intended access restrictions in the context of the affected application, and can cause the arbitrary command injection. Impact Level: Application

Solution
Upgrade to Apache HTTP Server version 2.2.15 or later For updates refer to http://www.apache.org/

Affected Software/OS
Apache HTTP Server on Linux.

Vulnerability Insight
The flaw is due to error in the mod_proxy_ftp module which can be exploited via vectors related to the embedding of these commands in the Authorization HTTP header.

Vulnerability Detection Method
Details:`Apache 'mod_proxy_ftp' Module Command Injection Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900842
Version used: `$Revision: 5390 $`

References
`CVE: CVE-2009-3095`
`BID:36254`
`Other:`
`URL:http://intevydis.com/vd-list.shtml`
`URL:http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html`

High (CVSS: 7.1)
NVT: Apache 'mod_proxy_http.c' Denial Of Service Vulnerability

Summary
This host is running Apache HTTP Server and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow remote attackers to cause Denial of Service to the legitimate user by CPU consumption. Impact Level: Application

Solution
Fixed in the SVN repository. http://svn.apache.org/viewvc?view=rev&revision=790587

Affected Software/OS
Apache HTTP Server version prior to 2.3.3

Vulnerability Insight
The flaw is due to error in 'stream_reqbody_cl' function in 'mod_proxy_http.c' in the mod_proxy module. When a reverse proxy is configured, it does not properly handle an amount of streamed data that exceeds the Content-Length value via crafted requests.

Vulnerability Detection Method
Details:Apache 'mod_proxy_http.c' Denial Of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800827
Version used: $Revision: 4865 $

References
CVE: CVE-2009-1890
BID:35565
Other:
URL:http://secunia.com/advisories/35691
URL:http://www.vupen.com/english/advisories/2009/1773
URL:http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=79058
↪6&pathrev=790587

High (CVSS: 10.0)
NVT: Apache Web Server End Of Life Detection (Linux)

Product detection result
cpe:/a:apache:http_server:1.3.37
Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004
↪98)

Summary
The Apache Web Server version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The Apache Web Server version has reached the end of life.
Installed version: 1.3.37
EOL version: 1.3
EOL date: 2010-02-03

... continues on next page ...

. . . continued from previous page . . .

Impact
An end of life version of Apache Web Server is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution
Solution type: VendorFix
Update the Apache Web Server version on the remote host to a still supported version.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is unsupported.
Details:`Apache Web Server End Of Life Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108085
Version used: `$Revision: 5928 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:1.3.37`
Method: `Apache Web Server Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
`Other:`
`URL:https://archive.apache.org/dist/httpd/Announcement1.3.html`
`URL:https://archive.apache.org/dist/httpd/Announcement2.0.html`
`URL:https://en.wikipedia.org/wiki/Apache_HTTP_Server#Versions`

High (CVSS: 7.5)
NVT: DataLife Engine 'catlist' Parameter PHP Code Injection Vulnerability

Summary
DataLife Engine is prone to a remote PHP code-injection vulnerability.
An attacker can exploit this issue to inject and execute arbitrary PHP code in the context of the affected application. This may facilitate a compromise of the application and the underlying system other attacks are also possible.
DataLife Engine 9.7 is vulnerable other versions may also be affected.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see the references for details.

Vulnerability Detection Method
Details:`DataLife Engine 'catlist' Parameter PHP Code Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103654

. . . continues on next page . . .

... continued from previous page ...

Version used: $Revision: 5699 $

References
CVE: CVE-2013-1412
BID:57603
Other:
URL:http://www.securityfocus.com/bid/57603

High (CVSS: 7.5)
NVT: GhostScripter Amazon Shop Multiple Vulnerabilities

Summary
Amazon Shop is prone to multiple vulnerabilities, including a cross-site scripting issue, a directory-traversal issue, and multiple remote file-include issues, because it fails to sufficiently sanitize user-supplied data.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45/info/search.php?query=1<script>alert(docume
↪nt.cookie);</script>&mode=all

Impact
An attacker can exploit these issues to run malicious PHP code in the context of the webserver process, run script code in an unsuspecting user's browser, steal cookie-based authentication credentials, or obtain sensitive information other attacks are also possible.

Vulnerability Detection Method
Details:GhostScripter Amazon Shop Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100024
Version used: $Revision: 4970 $

References
BID:33994

High (CVSS: 7.5)
NVT: Log1 CMS 'data.php' PHP Code Injection Vulnerability

Summary
Log1 CMS is prone to a remote PHP code-injection vulnerability.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45/info/admin/libraries/ajaxfilemanager/inc/da
↪ta.php

Impact

... continues on next page ...

... continued from previous page ...

An attacker can exploit this issue to inject and execute arbitrary PHP code in the context of the affected application. This may facilitate a compromise of the application and the underlying system other attacks are also possible.

Affected Software/OS
Log1 CMS 2.0 is vulnerable other versions may also be affected.

Vulnerability Detection Method
Details:`Log1 CMS 'data.php' PHP Code Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103496
Version used: `$Revision: 5715 $`

References
`CVE: CVE-2011-4825`
`BID:50523`
`Other:`
`URL:http://www.securityfocus.com/bid/50523`

High (CVSS: 7.5)
NVT: Netref Cat_for_gen.PHP Remote PHP Script Injection Vulnerability

Summary
The remote host is running the Netref directory script, written in PHP.
There is a vulnerability in the installed version of Netref that enables a remote attacker to pass arbitrary PHP script code through the 'ad', 'ad_direct', and 'm_for_racine' parameters of the 'cat_for_gen.php' script. This code will be executed on the remote host under the privileges of the web server userid.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/script/cat_for_gen.php?ad=1&ad_direct=`
`↪../&m_for_racine=%3C/option%3E%3C/SELECT%3E%3C?phpinfo();?%3E`

Solution
Solution type: VendorFix
Upgrade to Netref 4.3 or later.

Vulnerability Detection Method
Details:`Netref Cat_for_gen.PHP Remote PHP Script Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.18358
Version used: `$Revision: 6046 $`

References
`CVE: CVE-2005-1222`
`BID:13275`

High (CVSS: 7.5)
NVT: PHP 'libgd' Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.27/7.0.12

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Update to PHP version 5.6.27 or 7.0.12. For updates refer to http://www.php.net

Affected Software/OS
PHP versions 5.x through 5.6.26 and 7.0.x through 7.0.11 on Linux

Vulnerability Insight
The flaw exist due to an integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'libgd' Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.809338
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-7568
BID:93184
Other:

... continues on next page ...

... continued from previous page ...

URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php
URL:http://seclists.org/oss-sec/2016/q3/639
URL:https://bugs.php.net/bug.php?id=73003

High (CVSS: 10.0)
NVT: PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to stack buffer overflow vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.4.43

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the PHP process. Failed exploit attempts will likely crash the webserver.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 on Linux

Vulnerability Insight
Multiple flaws are due to - Inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script. - Improper validation of file pointer in the 'phar_convert_to_other' function in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (L...
OID:1.3.6.1.4.1.25623.1.0.807507
Version used: $Revision: 5083 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2015-5590, CVE-2015-8838, CVE-2015-5589
BID:75970, 88763, 75974
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:https://bugs.php.net/bug.php?id=69923

High (CVSS: 7.5)
NVT: PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to remote code execution vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.4.45

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely cause a denial-of-service condition.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Linux

Vulnerability Insight
The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Li.
↪..
OID:1.3.6.1.4.1.25623.1.0.807505
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2015-6836
BID:76644
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:https://bugs.php.net/bug.php?id=70388

High (CVSS: 7.5)
NVT: PHP 'substr_replace()' Use After Free Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is running PHP and is prone to Use After Free vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.7

Impact
Successful exploitation could allow remote attackers to execute arbitrary code in the context of a web server. Failed attempts will likely result in denial-of-service conditions.
Impact Level: Network

Solution
Solution type: VendorFix
Upgrade to PHP version 5.3.7 or later. For updates refer to http://www.php.net/downloads.php

Affected Software/OS

... continues on next page ...

... continued from previous page ...

PHP version 5.3.6 and prior.

Vulnerability Insight
The flaw is due to passing the same variable multiple times to the 'substr_replace()' function, which makes the PHP to use the same pointer in three variables inside the function.

Vulnerability Detection Method
Details:PHP 'substr_replace()' Use After Free Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902356
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2011-1148
BID:46843
Other:
URL:http://bugs.php.net/bug.php?id=54238
URL:http://openwall.com/lists/oss-security/2011/03/13/3

High (CVSS: 10.0)
NVT: PHP 'type confusion' Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.7

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to PHP version 5.6.7 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.7 on Linux

Vulnerability Insight
The flaw is due to 'type confusion' issues in 'ext/soap/php_encoding.c', 'ext/soap/php_http.c', and 'ext/soap/soap.c' scripts.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP 'type confusion' Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808673
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2015-4601`
`BID:75246`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 7.5)
NVT: PHP 'var_unserializer' Denial of Service Vulnerability (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.6.26`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.26, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.26 on Linux

Vulnerability Insight
The flaw is due to improper handling of object-deserialization failures in 'ext/standard/var_unserializer.re' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP 'var_unserializer' Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809321
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-7411`
`BID:93009`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 10.0)
NVT: PHP 5.2.0 and Prior Versions Multiple Vulnerabilities

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
PHP 5.2.0 and prior versions are prone to multiple security vulnerabilities. Successful exploits could allow an attacker to write files in unauthorized locations, cause a denial-of-service condition, and potentially execute code.

Vulnerability Detection Result
`Installed version: 4.4.4`

... continues on next page ...

... continued from previous page ...

Fixed version: 4.4.5/5.2.1

Solution
Solution type: VendorFix
The vendor has released updates to address these issues. Contact the vendor for details on obtaining and applying the appropriate updates.
Please see the advisories for more information.

Affected Software/OS
These issues are reported to affect PHP 4.4.4 and prior versions in the 4 branch, and 5.2.0 and prior versions in the 5 branch other versions may also be vulnerable.

Vulnerability Detection Method
Details:PHP 5.2.0 and Prior Versions Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100606
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, CVE-2007-0909,
↪CVE-2007-0910
BID:22496
Other:
URL:http://www.securityfocus.com/bid/22496
URL:http://support.avaya.com/elmodocs2/security/ASA-2007-136.htm
URL:http://www.php.net/ChangeLog-5.php#5.2.1
URL:http://www.php.net/releases/5_2_1.php
URL:http://support.avaya.com/elmodocs2/security/ASA-2007-101.htm
URL:http://rhn.redhat.com/errata/RHSA-2007-0076.html
URL:http://rhn.redhat.com/errata/RHSA-2007-0081.html#Red%20Hat%20Linux%20Adva
↪nced%20Workstation%202.1%20for%20the%20Itanium%20Processor
URL:http://rhn.redhat.com/errata/RHSA-2007-0082.html
URL:http://rhn.redhat.com/errata/RHSA-2007-0089.html
URL:http://www.novell.com/linux/security/advisories/2007_44_php.html

High (CVSS: 7.5)
NVT: PHP < 5.2.13 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

... continues on next page ...

... continued from previous page ...

Summary
The remote web server has installed a PHP Version which is prone to Multiple Vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.2.13`

Solution
Solution type: VendorFix
Updates are available. Please see the references for details.

Affected Software/OS
PHP versions prior to 5.2.13 are affected.

Vulnerability Insight
Multiple vulnerabilities exist due to:
1. A 'safe_mode' restriction-bypass vulnerability. Successful exploits could allow an attacker to write session files in arbitrary directions.
2. A 'safe_mode' restriction-bypass vulnerability. Successful exploits could allow an attacker to access files in unauthorized locations or create files in any writable directory.
3. An unspecified security vulnerability that affects LCG entropy.

Vulnerability Detection Method
Details:`PHP < 5.2.13 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100511
Version used: `$Revision: 4505 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2010-1128, CVE-2010-1129`
`BID:38182, 38431, 38430`
`Other:`
`URL:http://www.securityfocus.com/bid/38182`
`URL:http://www.securityfocus.com/bid/38431`
`URL:http://www.securityfocus.com/bid/38430`
`URL:http://securityreason.com/achievement_securityalert/82`
`URL:http://www.php.net/releases/5_2_13.php`
`URL:http://www.php.net`
`URL:http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/session/sessio`
`↪n.c?r1=293036&r2=294272`

... continues on next page ...

... continued from previous page ...

URL:http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/session/sessio
↪n.c?r1=293036&r2=294272

High (CVSS: 7.5)
NVT: PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to arbitrary code execution vulnerability

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.27

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.27, or 5.6.11, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.27 and 5.6.x before 5.6.11 on Linux.

Vulnerability Insight
The flaw is due to Use-after-free vulnerability in the 'spl_ptr_heap_insert' function in 'ext/spl/spl_heap.c'.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808671
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2015-4116
BID:75127
Other:
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 10.0)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.32

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.32, or 5.6.18, or 7.0.3, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 on Linux

Vulnerability Insight
The flaw is due an improper handling of zero-length uncompressed data in 'ext/phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808607
Version used: $Revision: 5083 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-4342, CVE-2016-2554
BID:89154, 83353
Other:
URL:http://www.php.net/ChangeLog-7.php
URL:http://www.openwall.com/lists/oss-security/2016/04/28/2

High (CVSS: 7.1)
NVT: PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.28

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (race condition and heap memory corruption) by leveraging an application that performs many temporary-file accesses.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.28, or 5.6.12, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.28 and 5.6.x before 5.6.12 on Linux

Vulnerability Insight
The flaw is due to script 'main/php_open_temporary_file.c' does not ensure thread safety.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808613
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2015-8878
BID:90837
Other:
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 7.5)
NVT: PHP Directory Traversal Vulnerability - Jul16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to Directory traversal vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.4.45

Impact
Successfully exploiting this issue allow remote attackers to read arbitrary empty directories, also to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 on Linux

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple flaws are due to - An error in the 'ZipArchive::extractTo' function in 'ext/zip/php_zip.c' script. - The xsl_ext_function_php function in ext/xsl/xsltprocessor.c when libxml2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop. - Improper handling of multiple php_var_unserialize calls. - Multiple use-after-free vulnerabilities.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Directory Traversal Vulnerability - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808617
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2014-9767, CVE-2015-6834, CVE-2015-6835, CVE-2015-6837, CVE-2015-6838`
`BID:76652, 76649, 76733, 76734, 76738`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:http://www.openwall.com/lists/oss-security/2016/03/16/20`

High (CVSS: 10.0)
NVT: PHP End Of Life Detection (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
The PHP version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.6/7.0`

Impact
An end of life version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update the PHP version on the remote host to a still supported version.

Affected Software/OS
PHP versions below PHP 5.6

Vulnerability Insight
Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have been reported are fixed and are released in regular point releases.
After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none, depending on the number of reports.
Once the three years of support are completed, the branch reaches its end of life and is no longer supported.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is unsupported.
Details:`PHP End Of Life Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.105889
Version used: `$Revision: 5580 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`Other:`
`URL:https://secure.php.net/supported-versions.php`

High (CVSS: 10.0)
NVT: PHP Heap-based buffer overflow in 'mbstring' extension

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
The host is running PHP and is prone to Buffer Overflow vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`

... continues on next page ...

... continued from previous page ...

Fixed version: 5.2.7

Impact
Successful exploitation could allow attackers to execute arbitrary code via a crafted string containing an HTML entity.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.7 or later, http://www.php.net/downloads.php

Affected Software/OS
PHP version 4.3.0 to 5.2.6 on all running platform.

Vulnerability Insight
The flaw is due to error in mbfilter_htmlent.c file in the mbstring extension. These can be exploited via mb_convert_encoding, mb_check_encoding, mb_convert_variables, and mb_parse_str functions.

Vulnerability Detection Method
Details:PHP Heap-based buffer overflow in 'mbstring' extension
OID:1.3.6.1.4.1.25623.1.0.900185
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-5557
BID:32948
Other:
URL:http://bugs.php.net/bug.php?id=45722
URL:http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0477.html

High (CVSS: 7.5)
NVT: PHP Imap_Mail_Compose() Function Buffer Overflow Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

... continues on next page ...

... continued from previous page ...

Summary
PHP is prone to a buffer-overflow vulnerability because the application fails to perform boundary checks before copying user-supplied data to insufficiently sized memory buffers.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 4.4.5`

Impact
An attacker can exploit this issue to execute arbitrary machine code in the context of the affected webserver. Failed exploit attempts will likely crash the webserver, denying service to legitimate users.

Solution
Solution type: VendorFix
The vendor released PHP 4.4.5 and 5.2.1 to address this issue. Please see the references for more information.

Affected Software/OS
This issue affects PHP versions prior to 4.4.5 and 5.2.1.

Vulnerability Detection Method
Details:`PHP Imap_Mail_Compose() Function Buffer Overflow Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100600
Version used: `$Revision: 4503 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2007-1825`
`BID:23234`
`Other:`
`URL:http://www.securityfocus.com/bid/23234`
`URL:http://www.php-security.org/MOPB/MOPB-40-2007.html`
`URL:http://www.php.net/`

High (CVSS: 7.5)
NVT: PHP Interruptions and Calltime Arbitrary Code Execution Vulnerability

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

... continues on next page ...

... continued from previous page ...

Summary
PHP is prone to a vulnerability that an attacker could exploit to execute arbitrary code with the privileges of the user running the affected application.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: N/A

Impact
Successful exploits will compromise the application and possibly the computer.

Vulnerability Detection Method
Details:PHP Interruptions and Calltime Arbitrary Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100252
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
BID:35867
Other:
URL:http://www.securityfocus.com/bid/35867
URL:http://www.php.net
URL:http://www.blackhat.com/presentations/bh-usa-09/ESSER/BHUSA09-Esser-PostE
↪xploitationPHP-PAPER.pdf

High (CVSS: 7.5)
NVT: PHP Msg_Receive() Memory Allocation Integer Overflow Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to an integer-overflow vulnerability because it fails to ensure that integer values aren't overrun. Attackers may exploit this issue to cause a buffer overflow and to corrupt process memory.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
Exploiting this issue may allow attackers to execute arbitrary machine code in the context of the affected application. Failed exploit attempts will likely result in a denial-of-service condition.

Solution
Solution type: VendorFix
Reports indicate that the vendor released version 4.4.5 and 5.2.1 to address this issue. Symantec has not confirmed this. Please contact the vendor for information on obtaining and applying fixes.

Affected Software/OS
This issue affects PHP versions prior to 4.4.5 and 5.2.1.

Vulnerability Detection Method
Details:PHP Msg_Receive() Memory Allocation Integer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100592
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1889
BID:23236
Other:
URL:http://www.securityfocus.com/bid/23236
URL:http://www.php-security.org/MOPB/MOPB-43-2007.html
URL:http://www.php.net/
URL:http://lists.suse.com/archive/suse-security-announce/2007-May/0007.html

High (CVSS: 7.5)
NVT: PHP Multiple Buffer Overflow Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary

... continues on next page ...

... continued from previous page ...

PHP is prone to multiple buffer-overflow vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.9

Impact
Successful exploits may allow attackers to execute arbitrary code in the context of applications using the vulnerable PHP functions. This may result in a compromise of the underlying system. Failed attempts may lead to a denial-of-service condition.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
Versions prior to PHP 4.4.9 and PHP 5.2.8 are vulnerable.

Vulnerability Detection Method
Details:PHP Multiple Buffer Overflow Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100583
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-3659, CVE-2008-3658
BID:30649
Other:
URL:http://www.securityfocus.com/bid/30649
URL:http://www.php.net/ChangeLog-5.php#5.2.8
URL:http://www.php.net/archive/2008.php#id2008-08-07-1
URL:http://www.php.net/
URL:http://support.avaya.com/elmodocs2/security/ASA-2009-161.htm

High (CVSS: 7.5)
NVT: PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.6.30`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (memory consumption or application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.30, 7.0.15 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.6.30 and 7.0.x before 7.0.15

Vulnerability Insight
Multiple flaws are due to - A integer overflow in the phar_parse_pharfile function in ext/phar/phar.c via a truncated manifest entry in a PHAR archive.
- A off-by-one error in the phar_parse_pharfile function in ext/phar/phar.c via a crafted PHAR archive with an alias mismatch.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:`PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108054
Version used: `$Revision: 5132 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-10159, CVE-2016-10160`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:http://www.php.net/ChangeLog-7.php`

High (CVSS: 7.5)
NVT: PHP Multiple Double Free Vulnerabilities - Jan15

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.21/5.6.5

Impact
Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.21 or 5.6.5 or later

Affected Software/OS
PHP versions through 5.5.20 and 5.6.x through 5.6.4

Vulnerability Insight
Multiple flaws are due to: - Double free error in the 'zend_ts_hash_graceful_destroy' function in 'zend_ts_hash.c script in the Zend Engine in PHP. - flaw in the 'GetCode_' function in 'gd_gif_in.c' script in GD Graphics Library (LibGD).

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Double Free Vulnerabilities - Jan15
OID:1.3.6.1.4.1.25623.1.0.805412
Version used: $Revision: 4498 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2014-9425, CVE-2014-9709
BID:71800, 73306

... continues on next page ...

... continued from previous page ...

Other:
URL:http://securitytracker.com/id/1031479
URL:https://bugs.php.net/bug.php?id=68676

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Apr16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.33

Impact
Successfully exploiting this issue allow remote attackers to gain access to potentially sensitive information and conduct a denial of service (memory corruption and application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.33 or 5.6.19 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.33, and 5.6.x before 5.6.19 on Linux

Vulnerability Insight
Multiple flaws are due to, - A use-after-free error in wddx.c script in the WDDX extension in PHP - An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 01 - Apr16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.807807
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.103592)

References

```
CVE: CVE-2016-3142, CVE-2016-3141
Other:
  URL:https://bugs.php.net/bug.php?id=71587
   URL:https://bugs.php.net/bug.php?id=71498
   URL:https://secure.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Aug16 (Linux)

Product detection result

```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     5.5.37
```

Impact

Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.
Impact Level: Application

Solution

Solution type: VendorFix
Upgrade to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later. For updates refer to http://www.php.net

Affected Software/OS

PHP versions prior to 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 on Linux

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple flaws are due to, - The 'php_zip.c' script in the zip extension improperly interacts with the unserialize implementation and garbage collection. - The php_wddx_process_data function in 'wddx.c' script in the WDDX extension mishandled data in a wddx_deserialize call. - The multiple integer overflows in 'mcrypt.c' script in the mcrypt extension. - The double free vulnerability in the '_php_mb_regex_ereg_replace_exec' function in 'php_mbregex.c' script in the mbstring extension. - An integer overflow in the '_gd2GetHeader' function in 'gd_gd2.c' script in the GD Graphics Library. - An integer overflow in the 'gdImageCreate' function in 'gd.c' script in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 01 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808788
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2016-5773, CVE-2016-5772, CVE-2016-5769, CVE-2016-5768, CVE-2016-5766,
↪CVE-2016-5767
BID:91397, 91398, 91399, 91396, 91395
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Jul16 (Linux)

Product detection result
```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.4.4
Fixed version:     5.5.34
```

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.34, or 5.6.20, or 7.0.5, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 on Linux

Vulnerability Insight
Multiple flaws are due to, - Multiple integer overflows in the mbfl_strcut function in 'ext/mbstring/libmbfl/mbfl/mbfilter.c' script. - A format string vulnerability in the php_snmp_error function in 'ext/snmp/snmp.c' script. - An improper handling of '\0' characters by the 'phar_analyze_path' function in 'ext/phar/phar.c' script. - An integer overflow in the 'php_raw_url_encode' function in 'ext/standard/url.c' script - An improper handling of continuation-level jumps in 'file_check_mem' function in 'funcs.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 01 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808199
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2015-8865`
`BID:85800, 85801, 85802, 85991, 85993`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:http://www.php.net/ChangeLog-7.php`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 01 - Mar16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.4.44`

Impact
Successfully exploiting this issue allow remote attackers to execute arbitrary code and to create or overwrite arbitrary files on the system and this may lead to launch further attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 on Linux

Vulnerability Insight
Multiple flaws are due to, - The multiple use-after-free vulnerabilities in SPL unserialize implementation. - An insufficient validation of user supplied input by 'phar/phar_object.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 01 - Mar16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807503
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2015-6831, CVE-2015-6832, CVE-2015-6833`
`BID:76737, 76739, 76735`
`Other:`
`URL:https://bugs.php.net/bug.php?id=70068`
`URL:http://www.openwall.com/lists/oss-security/2015/08/19/3`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Aug16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.37

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code or possibly have unspecified other impact via a large integer argument.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.37, or 5.6.23, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.37 and 5.6.x before 5.6.23 on Linux

Vulnerability Insight
Multiple flaws are due to, - The 'spl_array.c' in the SPL extension improperly interacts with the unserialize implementation and garbage collection. - The integer overflow in the 'SplFileObject::fread' function in 'spl_directory.c' in the SPL extension.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 02 - Aug16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808790
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-5771, CVE-2016-5770

... continues on next page ...

... continued from previous page ...

BID:91401, 91403
Other:
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Jan15

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple vulnerbilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.5

Impact
Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.5 or later

Affected Software/OS
PHP versions before 5.6.5

Vulnerability Insight
The flaw is due to a free operation on a stack-based character array by The apprentice_load function in libmagic/apprentice.c in the Fileinfo component.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 02 - Jan15
OID:1.3.6.1.4.1.25623.1.0.805413
Version used: $Revision: 4498 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2014-9426
Other:
URL:https://bugs.php.net/bug.php?id=68665
URL:http://securitytracker.com/id/1031480

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 02 - Sep16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.25

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory, to inject arbitrary-type session data by leveraging control of a session name.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.25, or 7.0.10, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.25 and 7.x before 7.0.10 on Linux

Vulnerability Insight
Multiple flaws are due to - An invalid wddxPacket XML document that is mishandled in a wddx_deserialize call in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_pop_element' function in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_process_data' function in 'ext/wddx/wddx.c' script. - Improper handling of the case of a thumbnail offset that exceeds the file size in 'exif_process_IFD_in_TIFF' function in 'ext/exif/exif.c' script. - Improper validation of gamma values in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - Improper validation of number of colors in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - The script 'ext/session/session.c' skips invalid session names in a way that triggers incorrect parsing. - Improper handling of certain objects in 'ext/standard/var_unserializer.c' script.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 02 - Sep16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.809319
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-7124, CVE-2016-7125, CVE-2016-7126, CVE-2016-7127, CVE-2016-7128,
↪CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132
BID:92756, 92552, 92755, 92757, 92564, 92758
Other:
URL:http://www.php.net/ChangeLog-7.php
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Aug16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.36

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.36, or 5.6.22, or later. For updates refer to http://www.php.net

Affected Software/OS

... continues on next page ...

... continued from previous page ...

PHP versions prior to 5.5.36 and 5.6.x before 5.6.22 on Linux

Vulnerability Insight
Multiple flaws are due to, - An integer overflow in the fread function in 'ext/standard/file.c' script. - An integer overflow in the php_html_entities function in 'ext/standard/html.c' script. - An Integer overflow in the php_escape_html_entities_ex function in 'ext/standard/html.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 03 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808792
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-5096 , CVE-2016-5094, CVE-2016-5095`
`BID:90861, 90857, 92144`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.5.35`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 on Linux.

Vulnerability Insight
The multiple flaws are due to, - An improper validation of TIFF start data in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper validation of IFD sizes in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper construction of spprintf arguments,in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An error in 'grapheme_strpos function' in 'ext/intl/grapheme/grapheme_string.c'. - An error in 'xml_parse_into_struct' function in 'ext/xml/xml.c' script. - The 'bcpowmod' function in 'ext/bcmath/bcmath.c' improperly modifies certain data structures. - An improper validation of input passed to 'bcpowmod' function in 'ext/bcmath/bcmath.c' script. - An error in 'grapheme_strpos' function in ext/intl/grapheme/grapheme_string.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 03 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808603
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541,
↪CVE-2016-4542, CVE-2016-4543, CVE-2016-4544
BID:89844, 90172, 90173, 90174
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 03 - Sep16 (Linux)

Product detection result
```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
```

... continues on next page ...

... continued from previous page ...

↪592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.6.26`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.25, or 7.0.10, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.25 and 7.x before 7.0.10 on Linux

Vulnerability Insight
Multiple flaws are due to, - Use-after-free vulnerability in the 'wddx_stack_destroy' function in 'ext/wddx/wddx.c' script. - Improper varification of a BIT field has the UNSIGNED_FLAG flag in 'ext/mysqlnd/mysqlnd_wireprotocol.c' script. - The ZIP signature-verification feature does not ensure that the uncompressed_filesize field is large enough. - The script 'ext/spl/spl_array.c' proceeds with SplArray unserialization without validating a return value and data type. - The script 'ext/intl/msgformat/msgformat_format.c' does not properly restrict the locale length provided to the Locale class in the ICU library. - An error in the php_wddx_push_element function in ext/wddx/wddx.c.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 03 - Sep16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809317
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417,`
↪`CVE-2016-7418`

... continues on next page ...

... continued from previous page ...

BID:93005, 93006, 93004, 93022, 93008, 93007, 93011
Other:
URL:http://www.php.net/ChangeLog-7.php
URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 04 - Aug16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.36

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 on Linux

Vulnerability Insight
Multiple flaws are due to, - The 'get_icu_value_internal' function in 'ext/intl/locale/locale_methods.c' script does not ensure the presence of a '\0' character. - The 'gd_interpolation.c' script in the GD Graphics Library mishandled by the imagescale function.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - 04 - Aug16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808794
Version used: $Revision: 5083 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2013-7456, CVE-2016-5093
BID:90946, 90859
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 04 - Jul16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.4.44

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution to defeat cryptographic protection mechanisms.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 on Linux

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The multiple flaws are due to, - An improper validation of certain Exception objects in 'Zend/zend_exceptions.c' script. - The 'openssl_random_pseudo_bytes' function in 'ext/openssl/openssl.c' incorrectly relies on the deprecated 'RAND_pseudo_bytes' function.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 04 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808604
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2015-8867, CVE-2015-8876, CVE-2015-8873, CVE-2015-8835
BID:87481, 90867, 84426, 90712
Other:
  URL:http://www.php.net/ChangeLog-5.php
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)

Product detection result
```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.4.4
Fixed version:     5.4.42
```

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service, to read or write to arbitrary files, also execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.
Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Linux

Vulnerability Insight
The multiple flaws are due to, - Improper validation of token extraction for table names, in the php_pgsql_meta_data function in pgsql.c in the PostgreSQL extension. - Integer overflow in the ftp_genlist function in ext/ftp/ftp.c - PHP does not ensure that pathnames lack %00 sequences.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808675
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2015-4644, CVE-2015-4643, CVE-2015-4598`
`BID:75291, 75292, 75244`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - 05 - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.5.38`

... continues on next page ...

... continued from previous page ...

Impact
Successfully exploiting this issue may allow attackers to cause a denial of service obtain sensitive information from process memory, or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.38, or 5.6.24, or 7.0.9, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 on Linux

Vulnerability Insight
Multiple flaws are due to - An integer overflow in the 'php_stream_zip_opener' function in 'ext/zip/zip_stream.c' script. - An integer signedness error in the 'simplestring_addn' function in 'simplestring.c' in xmlrpc-epi. - The 'ext/snmp/snmp.c' script improperly interacts with the unserialize implementation and garbage collection. - The 'locale_accept_from_http' function in 'ext/intl/locale/locale_methods.c' script does not properly restrict calls to the ICU 'uloc_acceptLanguageFromHTTP' function. - An error in the 'exif_process_user_comment' function in 'ext/exif/exif.c' script. - An error in the 'exif_process_IFD_in_MAKERNOTE' function in 'ext/exif/exif.c' script. - The 'ext/session/session.c' does not properly maintain a certain hash data structure. - An integer overflow in the 'virtual_file_ex' function in 'TSRM/tsrm_virtual_cwd.c' script. - An error in the 'php_url_parse_ex' function in 'ext/standard/url.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Vulnerabilities - 05 - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808634
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2016-6288, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292,
↪CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297
BID:92111, 92074, 92097, 92073, 92078, 92115, 92094, 92095, 92099
Other:
  URL:http://php.net/ChangeLog-5.php
   URL:http://php.net/ChangeLog-7.php
   URL:http://openwall.com/lists/oss-security/2016/07/24/2
```

High (CVSS: 10.0)
NVT: PHP Multiple Vulnerabilities - Aug08

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
The host is installed with PHP, that is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.6

Impact
Successful exploitation could result in remote arbitrary code execution, security restrictions bypass, access to restricted files, denial of service.
Impact Level: System

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.6 or above, http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.2.6

Vulnerability Insight
The flaws are caused by, - an unspecified stack overflow error in FastCGI SAPI (fastcgi.c). - an error during path translation in cgi_main.c. - an error with an unknown impact/attack vectors. - an unspecified error within the processing of incomplete multibyte characters in escapeshellcmd() API function. - error in curl/interface.c in the cURL library(libcurl), which could be exploited by attackers to bypass safe_mode security restrictions. - an error in PCRE. i.e buffer overflow error when handling a character class containing a very large number of characters with codepoints greater than 255(UTF-8 mode).

Vulnerability Detection Method
Details:PHP Multiple Vulnerabilities - Aug08
OID:1.3.6.1.4.1.25623.1.0.800110
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

. . . continues on next page . . .

... continued from previous page ...

References

```
CVE: CVE-2008-2050, CVE-2008-2051, CVE-2007-4850, CVE-2008-0599, CVE-2008-0674
BID:29009, 27413, 27786
Other:
  CB-A:08-0118
   URL:http://pcre.org/changelog.txt
   URL:http://www.php.net/ChangeLog-5.php
   URL:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0176
   URL:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0178
   URL:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0086
```

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - Dec09

Product detection result

```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary

This host is running PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     5.2.11
```

Impact

Successful exploitation could allow local attackers to bypass certain security restrictions and cause denial of service.
Impact Level: Network

Solution

Solution type: VendorFix
Upgrade to PHP version 5.3.1, http://www.php.net/downloads.php

Affected Software/OS

PHP version 5.2.10 and prior. PHP version 5.3.x before 5.3.1

Vulnerability Insight

Multiple flaws are due to: - Error in 'proc_open()' function in 'ext/standard/proc_open.c' that does not enforce the 'safe_mode_allowed_env_vars' and 'safe_mode_protected_env_vars' directives, which allows attackers to execute programs with an arbitrary environment via the env parameter. - Error in 'zend_restore_ini_entry_cb()' function in 'zend_ini.c', which allows attackers to obtain sensitive information.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Vulnerabilities - Dec09
OID:1.3.6.1.4.1.25623.1.0.801060
Version used: $Revision: 4504 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-4018, CVE-2009-2626
BID:37138, 36009
Other:
URL:http://secunia.com/advisories/37482
URL:http://bugs.php.net/bug.php?id=49026
URL:http://securityreason.com/achievement_securityalert/65
URL:http://www.openwall.com/lists/oss-security/2009/11/23/15

High (CVSS: 7.5)
NVT: PHP Multiple Vulnerabilities - Sep09

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is running PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.11

Impact
Successful exploitation will allow attackers to spoof certificates and can cause unknown impacts in the context of the web application.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.11 or later http://www.php.net/downloads.php

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP version prior to 5.2.11

Vulnerability Insight
- An error in 'php_openssl_apply_verification_policy' function that does not properly perform certificate validation. - An input validation error exists in the processing of 'exif' data. - An unspecified error exists related to the sanity check for the color index in the 'imagecolortransparent' function.

Vulnerability Detection Method
Details:`PHP Multiple Vulnerabilities - Sep09`
OID:1.3.6.1.4.1.25623.1.0.900871
Version used: `$Revision: 4505 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293`
`BID:36449`
`Other:`
`URL:http://secunia.com/advisories/36791`
`URL:http://www.php.net/releases/5_2_11.php`
`URL:http://www.php.net/ChangeLog-5.php#5.2.11`
`URL:http://www.openwall.com/lists/oss-security/2009/09/20/1`

High (CVSS: 7.5)
NVT: PHP Out of Bounds Read Multiple Vulnerabilities - Jan15

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.4.37/5.5.21/5.6.5`

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to obtain sensitive information and trigger unexpected code execution .
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later

Affected Software/OS
PHP versions through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4

Vulnerability Insight
The flaw is due to an out-of-bounds read error in sapi/cgi/cgi_main.c in the CGI component in PHP.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Out of Bounds Read Multiple Vulnerabilities - Jan15`
OID:1.3.6.1.4.1.25623.1.0.805414
Version used: `$Revision: 4498 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2014-9427`
`BID:71833`
`Other:`
`URL:https://bugs.php.net/bug.php?id=68618`

High (CVSS: 7.5)
NVT: PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
This host is installed with PHP and is prone to remote code execution vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 4.4.4
Fixed version:     5.3.28/5.4.23/5.5.7
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption).
Impact Level: Application

Solution
Solution type: VendorFix
Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7.

Vulnerability Insight
The flaw is due to a boundary error within the 'asn1_time_to_time_t' function in 'ext/openssl/openssl.c' when parsing X.509 certificates.

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13`
OID:1.3.6.1.4.1.25623.1.0.804174
Version used: `$Revision: 4500 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References

```
CVE: CVE-2013-6420
Other:
  URL:http://secunia.com/advisories/56055
   URL:http://packetstormsecurity.com/files/124436/PHP-openssl_x509_parse-Memory
↪-Corruption.html
```

High (CVSS: 7.5)
NVT: PHP Session Data Deserialization Arbitrary Code Execution Vulnerability

Product detection result

```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

... continues on next page ...

... continued from previous page ...

Summary
PHP is prone to an arbitrary-code-execution vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 4.4.5`

Impact
An attacker may exploit this issue to execute arbitrary code within the context of the affected webserver.

Solution
Solution type: VendorFix
Please see the references for more information.

Affected Software/OS
This issue affects PHP 4 versions prior to 4.4.5 and PHP 5 versions prior to 5.2.1.

Vulnerability Detection Method
Details:`PHP Session Data Deserialization Arbitrary Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100602
Version used: `$Revision: 4503 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2007-1701, CVE-2007-1700`
`BID:23120, 23119`
`Other:`
`URL:http://www.securityfocus.com/bid/23120`
`URL:http://www.securityfocus.com/bid/23119`
`URL:http://www8.itrc.hp.com/service/cki/docDisplay.do?docId=c01056506`
`URL:http://www.php-security.org/MOPB/MOPB-31-2007.html`
`URL:http://www.php.net`

High (CVSS: 7.5)
NVT: PHP Shared Memory Functions Resource Verification Arbitrary Code Execution Vulnerability

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
PHP shared memory functions (shmop) are prone to an arbitrary-code- execution vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
An attacker may exploit this issue to execute arbitrary code within the context of the affected webserver. The attacker may also gain access to RSA keys of the SSL certificate.

Solution
Solution type: VendorFix
The vendor released versions 4.4.5 and 5.2.1 to address this issue. Please see the references for more information.

Affected Software/OS
This issue affects PHP 4 versions prior to 4.4.5 and PHP 5 versions prior to 5.2.1.

Vulnerability Detection Method
Details:PHP Shared Memory Functions Resource Verification Arbitrary Code Execution Vuln..
OID:1.3.6.1.4.1.25623.1.0.100605
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1376
BID:22862
Other:
URL:http://www.securityfocus.com/bid/22862
URL:http://www.php-security.org/MOPB/MOPB-15-2007.html
URL:http://www.php.net
URL:http://lists.suse.com/archive/suse-security-announce/2007-May/0007.html

High (CVSS: 7.5)
NVT: PHP sqlite_udf_decode_binary() Function Buffer Overflow Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
PHP is prone to a buffer-overflow vulnerability because the application fails to perform boundary checks before copying user-supplied data to insufficiently sized memory buffers.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
An attacker can exploit this issue to execute arbitrary machine code in the context of the affected webserver. Failed exploit attempts will likely crash the webserver, denying service to legitimate users.

Solution
Solution type: VendorFix
Reports indicate that the vendor released versions 4.4.5 and 5.2.1 to address this issue. Please contact the vendor for information on obtaining and applying fixes.
The reporter of this issue indicates that if you are using a shared copy of an external Sqlite library, you will remain vulnerable to this issue, even after upgrading to nonvulnerable versions.

Affected Software/OS
This issue affects PHP versions prior to 4.4.5 and 5.2.1.

Vulnerability Detection Method
Details:PHP sqlite_udf_decode_binary() Function Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100593
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1888, CVE-2007-1887
BID:23235
Other:
URL:http://www.securityfocus.com/bid/23235

. . . continues on next page . . .

... continued from previous page ...

URL:http://www.php.net/ChangeLog-5.php#5.2.3
URL:http://www.php-security.org/MOPB/MOPB-41-2007.html
URL:http://www.php.net/
URL:http://www.securityfocus.com/archive/1/481830

High (CVSS: 7.5)
NVT: PHP Str_Replace() Integer Overflow Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to an integer-overflow vulnerability because it fails to ensure that integer values aren't overrun. Attackers may exploit this issue to cause a buffer-overflow and corrupt process memory.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
Exploiting this issue may allow attackers to execute arbitrary machine code in the context of the affected application. Failed exploit attempts will likely result in a denial-of-service condition.

Solution
Solution type: VendorFix
The vendor released PHP 4.4.5 and 5.2.1 to address this issue. Please see the references for more information.

Affected Software/OS
This issue affects versions prior to PHP 4.4.5 and 5.2.1.

Vulnerability Detection Method
Details:PHP Str_Replace() Integer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100594
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

References

CVE: CVE-2007-1885, CVE-2007-1886
BID:23233
Other:
URL:http://www.securityfocus.com/bid/23233
URL:http://www8.itrc.hp.com/service/cki/docDisplay.do?docId=c01056506
URL:http://www.php-security.org/MOPB/MOPB-39-2007.html
URL:http://www.php.net/releases/4_4_5.php
URL:http://www.php.net/releases/5_2_1.php
URL:http://www.php.net/

High (CVSS: 10.0)
NVT: PHP Version < 4.4.5 Multiple Vulnerabilities

Product detection result

cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary

PHP version smaller than 4.4.5 suffers from multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 4.4.4
Fixed version: 4.4.5

Solution

Solution type: VendorFix
Update PHP to version 4.4.5 or later.

Vulnerability Detection Method

Details:PHP Version < 4.4.5 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110174
Version used: $Revision: 4506 $

Product Detection Result

Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References

CVE: CVE-2006-4625, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908,
↪CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1286, CVE-2007-1376, CVE
↪-2007-1378, CVE-2007-1379, CVE-2007-1380, CVE-2007-1700, CVE-2007-1701, CVE-20
↪07-1777, CVE-2007-1825, CVE-2007-1835, CVE-2007-1884, CVE-2007-1885, CVE-2007-

... continues on next page ...

... continued from previous page ...

↪1886, CVE-2007-1887, CVE-2007-1890
BID:22496, 22805, 22806, 22833, 22862, 23119, 23120, 23169, 23219, 23233, 23234, ↪ 23235, 23236

High (CVSS: 7.5)
NVT: PHP Version < 4.4.8 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103 ↪592)

Summary
PHP version smaller than 4.4.8 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.8

Solution
Solution type: VendorFix
Update PHP to version 4.4.8 or later.

Vulnerability Detection Method
Details:PHP Version < 4.4.8 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110186
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-3378, CVE-2007-3997, CVE-2007-3799, CVE-2007-4657, CVE-2007-4658, ↪CVE-2008-0145, CVE-2008-2108
BID:24661, 49631

High (CVSS: 7.5)
NVT: PHP Version < 4.4.9 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4

... continues on next page ...

... continued from previous page ...

Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
PHP < 4.4.9 suffers from multiple vulnerabilities such as buffer overflow and DOS attack.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.9

Solution
Solution type: VendorFix
Upgrade to PHP version 4.4.9 or later.

Vulnerability Detection Method
Details:PHP Version < 4.4.9 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110068
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-4850, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2009-0754
BID:27413, 30649, 31612, 33542

High (CVSS: 9.3)
NVT: PHP Version < 5.1.2 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
PHP version smaller than 5.1.2 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.1.2

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Update PHP to version 5.1.2 or later.

Vulnerability Detection Method
Details:`PHP Version < 5.1.2 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.110177
Version used: `$Revision: 4506 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2006-0200, CVE-2006-0207, CVE-2006-0208`
`BID:16220, 16803`

High (CVSS: 10.0)
NVT: PHP Version < 5.2.0 Multiple Vulnerabilities

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
PHP version smaller than 5.2.0 suffers from multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.4.4
Fixed version:     5.2.0
```

Solution
Solution type: VendorFix
Update PHP to version 5.2.0 or later.

Vulnerability Detection Method
Details:`PHP Version < 5.2.0 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.110173
Version used: `$Revision: 4506 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`

... continues on next page ...

... continued from previous page ...

Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2006-1015, CVE-2006-1549, CVE-2006-2660, CVE-2006-4486, CVE-2006-4625, ↪CVE-2006-4812, CVE-2006-5465, CVE-2006-5706, CVE-2006-7205, CVE-2007-0448, CVE ↪-2007-1381, CVE-2007-1584, CVE-2007-1888, CVE-2007-2844, CVE-2007-5424
BID:20349, 20879, 49634

High (CVSS: 10.0)
NVT: PHP Version < 5.2.1 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103 ↪592)

Summary
PHP version smaller than 5.2.1 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.1

Solution
Solution type: VendorFix
Update PHP to version 5.2.1 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.1 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110175
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2006-6383, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, ↪CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1376, CVE-2007-1380, CVE ↪-2007-1383, CVE-2007-1452, CVE-2007-1453, CVE-2007-1454, CVE-2007-1700, CVE-20 ↪07-1701, CVE-2007-1824, CVE-2007-1825, CVE-2007-1835, CVE-2007-1884, CVE-2007- ↪1885, CVE-2007-1886, CVE-2007-1887, CVE-2007-1889, CVE-2007-1890, CVE-2007-444

... continues on next page ...

... continued from previous page ...

↪1, CVE-2007-4586
BID:21508, 22496, 22805, 22806, 22862, 22922, 23119, 23120, 23219, 23233, 23234,
↪ 23235, 23236, 23237, 23238

High (CVSS: 7.5)
NVT: PHP Version < 5.2.11 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.11 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.11

Solution
Solution type: VendorFix
Update PHP to version 5.2.11 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.11 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110176
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018,
↪CVE-2009-5016
BID:36449, 44889

High (CVSS: 9.3)
NVT: PHP Version < 5.2.14 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4

... continues on next page ...

... continued from previous page ...

Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.14 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.14

Solution
Solution type: VendorFix
Update PHP to version 5.2.14 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.14 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110171
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,
↪CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE
↪-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3065
BID:38708, 40948, 41991

High (CVSS: 7.8)
NVT: PHP Version < 5.2.2 Vulnerabilitiy

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.2 suffers from a vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4

... continues on next page ...

... continued from previous page ...

Fixed version: 5.2.2

Solution
Solution type: VendorFix
Update PHP to version 5.2.2 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.2 Vulnerabilitiy
OID:1.3.6.1.4.1.25623.1.0.110185
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1649
BID:23105

High (CVSS: 7.5)
NVT: PHP Version < 5.2.4 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.4 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.4

Solution
Solution type: VendorFix
Update PHP to version 5.2.4 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.4 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110184
Version used: $Revision: 4506 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1413, CVE-2007-2872, CVE-2007-3294, CVE-2007-3378, CVE-2007-3790,
↪CVE-2007-3799, CVE-2007-3806, CVE-2007-4010, CVE-2007-4033, CVE-2007-4255, CVE
↪-2007-4507, CVE-2007-4652, CVE-2007-4658, CVE-2007-4659, CVE-2007-4660, CVE-20
↪07-4661, CVE-2007-4662, CVE-2007-4663
BID:24661, 24261, 24922, 25498

High (CVSS: 9.3)
NVT: PHP Version < 5.2.5 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.5 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.5

Solution
Solution type: VendorFix
Update PHP to version 5.2.5 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.5 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110179
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-3996, CVE-2007-4782, CVE-2007-4783, CVE-2007-4784, CVE-2007-4825,
↪CVE-2007-4840, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE

... continues on next page ...

... continued from previous page ...

↪-2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2008-2107, CVE-2008-2108, CVE-20
↪08-4107
BID:26403

High (CVSS: 10.0)
NVT: PHP Version < 5.2.6 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.6 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.6

Solution
Solution type: VendorFix
Update PHP to version 5.2.6 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.6 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110183
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-4850, CVE-2007-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050,
↪CVE-2008-2051
BID:27413, 28392, 29009

High (CVSS: 10.0)
NVT: PHP Version < 5.2.7 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4

... continues on next page ...

... continued from previous page ...

Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.7 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.7

Solution
Solution type: VendorFix
Update PHP to version 5.2.7 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.7 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110172
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658,
↪CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE
↪-2008-5658
BID:29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948

High (CVSS: 7.5)
NVT: PHP Version < 5.2.8 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.8 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4

... continues on next page ...

... continued from previous page ...

Fixed version: 5.2.8

Solution
Solution type: VendorFix
Update PHP to version 5.2.8 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.8 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110180
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-5814, CVE-2008-5844
BID:32673

High (CVSS: 7.5)
NVT: PHP Version < 5.3.1 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.3.1 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.1

Solution
Solution type: VendorFix
Update PHP to version 5.3.1 or later.

Vulnerability Detection Method
Details:PHP Version < 5.3.1 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110178
Version used: $Revision: 4506 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-3557, CVE-2009-3559, CVE-2009-4017, CVE-2009-4018, CVE-2010-1128
BID:36554, 36555, 37079, 37138

High (CVSS: 9.3)
NVT: PHP Version < 5.3.3 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.3.3 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.3

Solution
Solution type: VendorFix
Update PHP to version 5.3.3 or later.

Vulnerability Detection Method
Details:PHP Version < 5.3.3 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110182
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,
↪CVE-2010-1917, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE
↪-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3062, CVE-20
↪10-3063, CVE-2010-3064, CVE-2010-3065
BID:38708, 40461, 40948, 41991

High (CVSS: 7.5)
NVT: PHP Versions Prior to 5.3.1 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
PHP is prone to multiple security vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.2

Impact
Some of these issues may be exploited to bypass security restrictions and create arbitrary files or cause denial-of-service conditions. The impact of the other issues has not been specified.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
These issues affect PHP versions prior to 5.3.1.

Vulnerability Detection Method
Details:PHP Versions Prior to 5.3.1 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100359
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
BID:37079
Other:
URL:http://www.securityfocus.com/bid/37079
URL:http://securityreason.com/securityalert/6601
URL:http://securityreason.com/securityalert/6600
URL:http://www.php.net/releases/5_3_1.php
URL:http://www.php.net/
URL:http://seclists.org/fulldisclosure/2009/Nov/228
URL:http://www.securityfocus.com/archive/1/507982

High (CVSS: 7.5)
NVT: PHP Zip_Entry_Read() Integer Overflow Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
PHP is prone to an integer-overflow vulnerability because it fails to ensure that integer values aren't overrun. Attackers may exploit this issue to cause a heap-based buffer overflow.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
Exploiting this issue may allow attackers to execute arbitrary machine code in the context of the affected application. Failed exploit attempts will likely result in a denial-of-service condition.

Solution
Solution type: VendorFix
Reports indicate that PHP 4.4.5 addresses this issue. Please contact the vendor for more information.

Affected Software/OS
This issue affects versions prior to PHP 4.4.5.

Vulnerability Detection Method
Details:PHP Zip_Entry_Read() Integer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100601
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1777
BID:23169
Other:
URL:http://www.securityfocus.com/bid/23169
URL:http://www.php-security.org/MOPB/MOPB-35-2007.html
URL:http://www.php.net/

High (CVSS: 9.0)
NVT: php-Charts 'index.php' Arbitrary PHP Code Execution Vulnerability

Summary
php-Charts is prone to an arbitrary PHP code-execution vulnerability.
An attacker can exploit this issue to execute arbitrary PHP code within the context of the affected application.
php-Charts 1.0 is vulnerable other versions may also be affected.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/wizard/index.php?type=';phpinfo();//`

Vulnerability Detection Method
Details:`php-Charts 'index.php' Arbitrary PHP Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103715
Version used: `$Revision: 5699 $`

References
`BID:59987`
`Other:`
`URL:http://www.securityfocus.com/bid/59987`

High (CVSS: 9.0)
NVT: php-Charts 'url.php' Arbitrary PHP Code Execution Vulnerability

Summary
php-Charts is prone to an arbitrary PHP code-execution vulnerability.
An attacker can exploit this issue to execute arbitrary PHP code within the context of the web server.
php-Charts 1.0 is vulnerable other versions may also be affected.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/wizard/url.php?${phpinfo()}=1`

Vulnerability Detection Method
Details:`php-Charts 'url.php' Arbitrary PHP Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103644
Version used: `$Revision: 5699 $`

References
`BID:57448`
`Other:`
`URL:http://www.securityfocus.com/bid/57448`

... continues on next page ...

... continued from previous page ...

High (CVSS: 7.5)
NVT: PHP-Nuke Multiple Vulnerabilities

Product detection result
cpe:/a:phpnuke:php-nuke
Detected by PHP-Nuke Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900338)

Summary
The host is running PHP-Nuke and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45

Impact
Successful exploitation will allow attacker to execute arbitrary SQL commands, inject arbitrary web script or hijack the authentication of administrators.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
PHP-Nuke versions 8.0 and prior.

Vulnerability Insight
Multiple flaws are due to, - An improper validation of user-supplied input to 'chng_uid', 'sender_name' and 'sender_email' parameter in the 'admin.php' and 'modules.php'. - An improper validation of user-supplied input to add user accounts or grant the administrative privilege in the 'mainfile.php'.

Vulnerability Detection Method
Details:PHP-Nuke Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.902600
Version used: $Revision: 5351 $

Product Detection Result
Product: cpe:/a:phpnuke:php-nuke
Method: PHP-Nuke Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900338)

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2011-1480, CVE-2011-1481, CVE-2011-1482
BID:47000, 47001, 47002
Other:
URL:http://xforce.iss.net/xforce/xfdb/66278
URL:http://xforce.iss.net/xforce/xfdb/66279
URL:http://xforce.iss.net/xforce/xfdb/66280

High (CVSS: 7.5)
NVT: PHP-Nuke Multiple Vulnerabilities

Product detection result
cpe:/a:phpnuke:php-nuke
Detected by PHP-Nuke Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900338)

Summary
The host is running PHP-Nuke and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45

Impact
Successful exploitation will allow attacker to execute arbitrary SQL commands, inject arbitrary web script or hijack the authentication of administrators.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
PHP-Nuke versions 8.0 and prior.

Vulnerability Insight
Multiple flaws are due to, - An improper validation of user-supplied input to 'chng_uid', 'sender_name' and 'sender_email' parameter in the 'admin.php' and 'modules.php'. - An improper validation of user-supplied input to add user accounts or grant the administrative privilege in the 'mainfile.php'.

Vulnerability Detection Method
Details:PHP-Nuke Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.902600
Version used: $Revision: 5351 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:phpnuke:php-nuke
Method: PHP-Nuke Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900338)

References
CVE: CVE-2011-1480, CVE-2011-1481, CVE-2011-1482
BID:47000, 47001, 47002
Other:
URL:http://xforce.iss.net/xforce/xfdb/66278
URL:http://xforce.iss.net/xforce/xfdb/66279
URL:http://xforce.iss.net/xforce/xfdb/66280

High (CVSS: 7.5)
NVT: phpBB Forum ID Security Bypass Vulnerability

Summary
phpBB is prone to a security-bypass vulnerability.
Attackers can exploit this vulnerability to bypass certain security restrictions and gain unauthorized access to the affected application.
Versions prior to phpBB 3.0.5 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:phpBB Forum ID Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100463
Version used: $Revision: 5394 $

References
CVE: CVE-2010-1630
BID:37882
Other:
URL:http://www.securityfocus.com/bid/37882
URL:http://www.phpbb.com/community/viewtopic.php?f=14&p=9764445
URL:http://www.phpbb.com/

High (CVSS: 7.5)
NVT: phpBB Forum ID Security Bypass Vulnerability

... continues on next page ...

... continued from previous page ...

Summary
phpBB is prone to a security-bypass vulnerability.
Attackers can exploit this vulnerability to bypass certain security restrictions and gain unauthorized access to the affected application.
Versions prior to phpBB 3.0.5 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:phpBB Forum ID Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100463
Version used: $Revision: 5394 $

References
CVE: CVE-2010-1630
BID:37882
Other:
URL:http://www.securityfocus.com/bid/37882
URL:http://www.phpbb.com/community/viewtopic.php?f=14&p=9764445
URL:http://www.phpbb.com/

High (CVSS: 7.5)
NVT: phpinfo() output accessible

Summary
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often times left in webserver directory after completion.

Vulnerability Detection Result
The following files are calling the function phpinfo() which disclose potentially sensitive information to the remote attacker:
http://192.168.27.45/info.php
http://192.168.27.45/webexploitation_package_02/webnews/phpinfo.php
http://192.168.27.45/info/phpinfo.php
http://192.168.27.45/info/info.php
http://192.168.27.45/info/test.php
http://192.168.27.45/info/php_info.php
http://192.168.27.45/info/index.php
http://192.168.27.45/webexploitation_package_01/info.php

Impact

... continues on next page ...

... continued from previous page ...

Some of the information that can be gathered from this file includes: The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, the system version(unix / linux), and the root directory of the web server.

Solution
Solution type: Workaround
Delete them or restrict access to the listened files.

Vulnerability Detection Method
Details:`phpinfo() output accessible`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `$Revision: 5815 $`

High (CVSS: 7.5)
NVT: PHPMoAdmin Unauthorized Remote Code Execution

Summary
PHPMoAdmin is prone to a remote code-execution vulnerability because the application fails to sufficiently sanitize user-supplied input.

Vulnerability Detection Result
```
Vulnerable url: http://192.168.27.45/info/moadmin.php?db=admin&action=listRows&c
↪ollection=fdsa&find=array();phpinfo();
```

Impact
Exploiting this issue will allow attackers to execute arbitrary code within the context of the affected application.

Solution
Solution type: NoneAvailable
Ask the Vendor for an update.

Vulnerability Detection Method
Send a special crafted HTTP GET request and check the response
Details:`PHPMoAdmin Unauthorized Remote Code Execution`
OID:1.3.6.1.4.1.25623.1.0.105230
Version used: `$Revision: 5819 $`

References
```
CVE: CVE-2015-2208
Other:
  URL:http://www.exploit-db.com/exploits/36251/
```

... continues on next page ...

... continued from previous page ...

High (CVSS: 8.5)
NVT: phpMyAdmin 'server_databases.php' Remote Command Execution Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to Remote Command Execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows execution of arbitrary commands, and possibly compromise the affected application. Impact Level : Application

Solution
Upgrade to phpMyAdmin 2.11.9.1 or newer http://www.phpmyadmin.net/home_page/downloads.php#2.11.9.1

Affected Software/OS
phpMyAdmin versions prior to 2.11.9.1 on all platform

Vulnerability Insight
This issue is caused by, sort_by parameter in server_databases.php which is not properly sanitised before being used.

Vulnerability Detection Method
Details:phpMyAdmin 'server_databases.php' Remote Command Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900130
Version used: $Revision: 4522 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2008-4096
BID:31188
Other:
URL:http://comments.gmane.org/gmane.comp.security.oss.general/947?set_lines=10
↪0000
URL:http://fd.the-wildcat.de/pma_e36a091q11.php

... continues on next page ...

... continued from previous page ...

URL:http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2008-7
URL:http://www.securityfocus.com/bid/31188/exploit

High (CVSS: 7.5)
NVT: phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to multiple input-validation vulnerabilities, including an HTTP response-splitting vulnerability and a local file-include vulnerability.
These issues can be leveraged to view or execute arbitrary local scripts, or misrepresent how web content is served, cached, or interpreted. This could aid in various attacks that try to entice client users into a false sense of trust. Other attacks are also possible.
Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100078
Version used: $Revision: 5016 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
BID:34253
Other:
URL:http://www.securityfocus.com/bid/34253

High (CVSS: 10.0)
NVT: phpMyAdmin Insecure Temporary File and Directory Creation Vulnerabilities

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin creates temporary directories and files in an insecure way.
An attacker with local access could potentially exploit this issue to perform symbolic-link attacks, overwriting arbitrary files in the context of the affected application.
Successful attacks may corrupt data or cause denial-of-service conditions. Other unspecified attacks are also possible.
This issue affects phpMyAdmin 2.11.x (prior to 2.11.10.)

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:phpMyAdmin Insecure Temporary File and Directory Creation Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100450
Version used: $Revision: 5394 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2008-7251, CVE-2008-7252
BID:37826
Other:
URL:http://www.securityfocus.com/bid/37826
URL:http://www.phpmyadmin.net/home_page/index.php
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-1.php
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-2.php

High (CVSS: 10.0)
NVT: WordPress 'wp-admin' Multiple Vulnerabilities - Aug09

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary

... continues on next page ...

... continued from previous page ...

The host is running WordPress and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue by sending malicious request to several scripts in the wp-admin directory to gain access to administrative functions which may allow them to obtain sensitive information or elevate privileges. Impact Level: System/Application

Solution
Update to Version 2.8.3 http://wordpress.org/download/

Affected Software/OS
WordPress version prior to 2.8.3 on all running platform.

Vulnerability Insight
- Application fails to properly sanitize user supplied input via a direct request to admin-footer.php, edit-category-form.php, edit-form-advanced.php, edit-form-comment.php, edit-link-category-form.php, edit-link-form.php, edit-page-form.php, and edit-tag-form.php in wp-admin/.
- Application fails to check capabilities for certain actions, it can be exploited to cause unauthorized edits or additions via a direct request to edit-comments.php, edit-pages.php, import.php, edit-category-form.php, edit-link-category-form.php, edit-tag-form.php, export.php, link-add.php or edit.php in wp-admin/.

Vulnerability Detection Method
Details:`WordPress 'wp-admin' Multiple Vulnerabilities - Aug09`
OID:1.3.6.1.4.1.25623.1.0.900915
Version used: `$Revision: 5148 $`

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:1.5.1.1`
Method: `WordPress Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
```
CVE: CVE-2009-2853, CVE-2009-2854
BID:35935
Other:
  URL:http://core.trac.wordpress.org/changeset/11768
   URL:http://core.trac.wordpress.org/changeset/11769
   URL:http://wordpress.org/development/2009/08/wordpress-2-8-3-security-release
↪/
```

High (CVSS: 8.5)
NVT: WordPress 'wp-admin/options.php' Remote Code Execution Vulnerability

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
The host is running WordPress and is prone to Remote Code Execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows remote attackers to execute arbitrary code by uploading a PHP script and adding this script pathname to active_plugins. Impact Level: System/Application

Solution
Upgrade to version 1.3.2 and 2.3.3 or later http://mu.wordpress.org/download/

Affected Software/OS
WordPress, WordPress prior to 2.3.3 WordPress, WordPress MU prior to 1.3.2

Vulnerability Insight
The flaw is due to error under 'wp-admin/options.php' file. These can be exploited by using valid user credentials with 'manage_options' and upload_files capabilities.

Vulnerability Detection Method
Details:WordPress 'wp-admin/options.php' Remote Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900183
Version used: $Revision: 4557 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
CVE: CVE-2008-5695
BID:27633
Other:
URL:http://secunia.com/advisories/28789
URL:http://www.milw0rm.com/exploits/5066
URL:http://mu.wordpress.org/forums/topic.php?id=7534&page&replies=1

High (CVSS: 7.5)
NVT: WordPress < 4.7.2 Multiple Security Vulnerabilities (Linux)

Product detection result
`cpe:/a:wordpress:wordpress:1.5.1.1`
`Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)`

Summary
This host is running WordPress and is prone to multiple security vulnerabilities because it fails to sanitize user-supplied input.

Vulnerability Detection Result
`Installed version: 1.5.1.1`
`Fixed version: 4.7.2`

Impact
Successfully exploiting this issue allow remote attacker to e.g. obtain sensitive information or inject arbitrary web script or HTML.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to WordPress version 4.7.2. For updates refer to https://wordpress.org

Affected Software/OS
WordPress versions 4.7.1 and earlier.

Vulnerability Insight
Multiple flaws are due to:
- The user interface for assigning taxonomy terms in Press This is shown to users who do not have permissions to use it.
- P_Query is vulnerable to a SQL injection (SQLi) when passing unsafe data. WordPress core is not directly vulnerable to this issue, but hardening was added to prevent plugins and themes from accidentally causing a vulnerability.
- A cross-site scripting (XSS) vulnerability was discovered in the posts list table.
- An unauthenticated privilege escalation vulnerability was discovered in a REST API endpoint.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:`WordPress < 4.7.2 Multiple Security Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108068
Version used: `$Revision: 5864 $`

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:1.5.1.1`
Method: `WordPress Version Detection`

. . . continues on next page . . .

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.900182)

References

```
CVE: CVE-2017-5610, CVE-2017-5611, CVE-2017-5612, CVE-2017-1001000
Other:
  URL:https://make.wordpress.org/core/2017/02/01/disclosure-of-additional-securi
↪ty-fix-in-wordpress-4-7-2/
   URL:https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/
   URL:https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress
↪-rest-api.html
   URL:http://www.secpod.com/blog/wordpress-rest-api-zero-day-privilege-escalati
↪on-vulnerability
```

High (CVSS: 9.3)
NVT: WordPress cat Parameter Directory Traversal Vulnerability

Product detection result

```
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)
```

Summary

The host is installed with WordPress and is prone to Directory Traversal Vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful attack could lead to execution of arbitrary PHP code and can even access sensitive information. Impact Level: Application

Solution

Solution type: VendorFix

Update to Version 2.5.1 or later. http://wordpress.org/

Affected Software/OS

WordPress 2.3.3 and earlier.

Vulnerability Insight

The flaw is due to improper validation of input passed via cat parameter to index.php which is not properly sanitized in the get_category_template() function.

Vulnerability Detection Method

Details:`WordPress cat Parameter Directory Traversal Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800124

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 4227 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
CVE: CVE-2008-4769
BID:28845
Other:
URL:http://secunia.com/advisories/29949
URL:http://www.juniper.fi/security/auto/vulnerabilities/vuln28845.html

High (CVSS: 7.5)
NVT: WordPress Multiple Vulnerabilities

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
This host is running WordPress, which is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to reset the password of arbitrary accounts, guess randomly generated passwords, obtain sensitive information and possibly to impersonate users and tamper with network data. Impact Level : Application

Solution
Solution type: VendorFix
Upgrade to WordPress 2.6.2 or later. http://wordpress.org/

Affected Software/OS
WordPress 2.6.1 and prior versions.

Vulnerability Insight
The flaws are due to, - SQL column-truncation issue. - Weakness in the entropy of generated passwords. - functions get_edit_post_link(), and get_edit_comment_link() fail to use SSL when transmitting data.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:WordPress Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.900219
Version used: $Revision: 4557 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
CVE: CVE-2008-3747
BID:30750, 31068, 31115
Other:
URL:http://www.sektioneins.de/advisories/SE-2008-05.txt
URL:http://seclists.org/fulldisclosure/2008/Sep/0194.html
URL:http://www.juniper.net/security/auto/vulnerabilities/vuln31068.html
URL:http://www.juniper.net/security/auto/vulnerabilities/vuln30750.html

High (CVSS: 7.5)
NVT: WordPress Multiple Vulnerabilities Dec15 (Linux)

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
This host is running WordPress and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed Version: 1.5.1.1
Fixed Version: 4.2.4

Impact
Successfully exploiting will allow remote attackers to inject arbitrary web script code in a user's browser session within the trust relationship between their browser and the server, to inject or manipulate SQL queries in the back-end database and to cause denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to WordPress version 4.2.4 or later, For updates refer to https://wordpress.org

Affected Software/OS

... continues on next page ...

... continued from previous page ...

WordPress Versions before 4.2.4 on linux.

Vulnerability Insight
Multiple flaws are due to, - An error in the legacy theme preview implementation within the file 'wp-includes/theme.php', which is not properly handling the user input. - An error in the function 'refreshAdvancedAccessibilityOfItem' within file 'wp-admin/js/nav-menu.js', which is not properly handling the user input. - An error in the function 'WP_Nav_Menu_Widget' class within file 'wp-includes/default-widgets.php', which is not properly handling the user input. - The function 'wp_untrash_post_comments' is not properly handling a comment after retrieving from trash within the file 'wp-includes/post.php' - The no usage of constant time comaprision for widgets in function 'sanitize_widget_instance' leads to timing side-channel attack by measuring the delay before inequality is calculated which is within the file 'wp-includes/class-wp-customize-widgets.php' - The Cross-site request forgery (CSRF) vulnerability in 'wp-admin/post.php'

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`WordPress Multiple Vulnerabilities Dec15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806801
Version used: `$Revision: 5087 $`

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:1.5.1.1`
Method: `WordPress Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
```
CVE: CVE-2015-5734, CVE-2015-5733, CVE-2015-5732, CVE-2015-5731, CVE-2015-5730,
↪CVE-2015-2213
BID:76331, 76160
Other:
  URL:http://seclists.org/oss-sec/2015/q3/290
   URL:https://wordpress.org/news/2015/08/wordpress-4-2-4-security-and-maintenan
↪ce-release/
```

[return to 192.168.27.45]

2.1.4 Medium general/tcp

Medium (CVSS: 6.4)
NVT: Adobe Flash Player Multiple Security Bypass Vulnerabilities - 01 Feb14 (Linux)

Product detection result
```
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)
```

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Adobe Flash Player and is prone to multiple security bypass vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to bypass certain security restrictions and disclose potentially sensitive information.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.346 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.346 on Linux.

Vulnerability Insight
Flaw are due to multiple unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Flash Player Multiple Security Bypass Vulnerabilities - 01 Feb14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804516
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:flash_player:9.0.31.0`
Method: `Adobe Flash Player/AIR Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
```
CVE: CVE-2014-0503, CVE-2014-0504
BID:66122, 66127
Other:
  URL:http://secunia.com/advisories/57271
   URL:http://helpx.adobe.com/security/products/flash-player/apsb14-08.html
```

Medium (CVSS: 6.4)
NVT: Adobe Flash Player Multiple Security Bypass Vulnerabilities - 01 Feb14 (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:adobe:flash_player:9.0.31.0
Detected by Adobe Flash Player/AIR Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800032)

Summary
This host is installed with Adobe Flash Player and is prone to multiple security bypass vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to bypass certain security restrictions and disclose potentially sensitive information.
Impact Level: System/Application

Solution
Solution type: VendorFix
Update to Adobe Flash Player version 11.2.202.346 or later, For updates refer to http://get.adobe.com/flashplayer

Affected Software/OS
Adobe Flash Player version before 11.2.202.346 on Linux.

Vulnerability Insight
Flaw are due to multiple unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Flash Player Multiple Security Bypass Vulnerabilities - 01 Feb14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804516
Version used: $Revision: 3521 $

Product Detection Result
Product: cpe:/a:adobe:flash_player:9.0.31.0
Method: Adobe Flash Player/AIR Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800032)

References
CVE: CVE-2014-0503, CVE-2014-0504
BID:66122, 66127
Other:
URL:http://secunia.com/advisories/57271
URL:http://helpx.adobe.com/security/products/flash-player/apsb14-08.html

Medium (CVSS: 4.3)
NVT: Adobe Flash Player Unspecified Cross-Site Scripting Vulnerability June-2011 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to cross-site scripting vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. Impact Level: Application/System

Solution
Upgrade to Adobe Flash Player version 10.3.181.22 or later. For updates refer to http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player versions before 10.3.181.22 on Linux.

Vulnerability Insight
The flaw is caused by improper validation of certain unspecified input, which allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Vulnerability Detection Method
Details:`Adobe Flash Player Unspecified Cross-Site Scripting Vulnerability June-2011 (Li.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.802205
Version used: `$Revision: 5424 $`

References
```
CVE: CVE-2011-2107
BID:48107
Other:
  URL:http://www.adobe.com/support/security/bulletins/apsb11-13.html
```

Medium (CVSS: 4.3)
NVT: Adobe Flash Player Unspecified Cross-Site Scripting Vulnerability June-2011 (Linux)

Summary
This host is installed with Adobe Flash Player and is prone to cross-site scripting vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. Impact Level: Application/System

Solution
Upgrade to Adobe Flash Player version 10.3.181.22 or later. For updates refer to http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player versions before 10.3.181.22 on Linux.

Vulnerability Insight
The flaw is caused by improper validation of certain unspecified input, which allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Vulnerability Detection Method
Details:`Adobe Flash Player Unspecified Cross-Site Scripting Vulnerability June-2011 (Li.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.802205
Version used: `$Revision: 5424 $`

References
`CVE: CVE-2011-2107`
`BID:48107`
`Other:`
`URL:http://www.adobe.com/support/security/bulletins/apsb11-13.html`

Medium (CVSS: 4.3)
NVT: Adobe Products Unspecified Cross-Site Scripting Vulnerability June-2011 (Windows)

Product detection result
`cpe:/a:adobe:acrobat_reader:7.0.5`
`Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0`
`↪.800108)`

Summary
This host is installed with Adobe Flash Player, Adobe Reader or Acrobat and is prone to cross-site scripting vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site.
Impact Level: Application/System

... continues on next page ...

... continued from previous page ...

Solution
Upgrade to Adobe Flash Player version 10.3.181.22 or later. For details refer, http://www.adobe.com/downloads/

Affected Software/OS
Adobe Flash Player versions prior to 10.3.181.22 on Windows. Adobe Reader and Acrobat X versions 10.0.3 and prior on Windows.

Vulnerability Insight
The flaw is caused by improper validation of certain unspecified input, which allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Products Unspecified Cross-Site Scripting Vulnerability June-2011 (Window.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.802206
Version used: `$Revision: 5424 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
`CVE: CVE-2011-2107`
`BID:48107`
`Other:`
`URL:http://www.adobe.com/support/security/bulletins/apsb11-13.html`

Medium (CVSS: 4.3)
NVT: Adobe Reader 'file://' URL Information Disclosure Vulnerability Feb07 (Linux)

Product detection result
`cpe:/a:adobe:acrobat_reader:7.0.5`
`Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0`
`↪.800108)`

Summary
This host is installed with Adobe Reader and is prone to information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow attackers to obtain sensitive information.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader version 8.1.2 or later. For updates refer to http://get.adobe.com/reader

Affected Software/OS
Adobe Reader version 8 and prior on Linux.

Vulnerability Insight
Flaw is due to some unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Reader 'file://' URL Information Disclosure Vulnerability Feb07 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804382
Version used: `$Revision: 3517 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
`CVE: CVE-2007-1199`
`BID:22753`
`Other:`
`URL:http://secunia.com/advisories/24408`
`URL:http://xforce.iss.net/xforce/xfdb/32815`

Medium (CVSS: 5.0)
NVT: Adobe Reader Cross-Site Scripting & Denial of Service Vulnerabilities (Linux)

Product detection result
`cpe:/a:adobe:acrobat_reader:7.0.5`
`Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0`
`↪.800108)`

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with Adobe Reader and is prone to cross site scripting and denial of service vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to cause memory corruption, conduct denial of service attack and the execution of arbitrary script code in a user's browser session in context of an affected site.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader version 9.2 or 8.1.7 or 7.1.4 or 7.0.9 or later. For updates refer to http://get.adobe.com/reader

Affected Software/OS
Adobe Reader version 9.x before 9.2, 8.x before 8.1.7, 7.x before 7.1.4, 7.0.8 and earlier on Linux.

Vulnerability Insight
Flaws exist due to, - the browser plug-in does not validate user supplied input to the hosted PDF file before returning the input to the user. - some unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Adobe Reader Cross-Site Scripting & Denial of Service Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804397
Version used: `$Revision: 3521 $`

Product Detection Result
Product: `cpe:/a:adobe:acrobat_reader:7.0.5`
Method: `Adobe products version detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
`CVE: CVE-2007-0045, CVE-2007-0048`
`BID:21858`
`Other:`
`URL:http://secunia.com/advisories/36983`
`URL:http://securitytracker.com/id?1017469`
`URL:http://www.adobe.com/support/security/bulletins/apsb07-01.html`
`URL:http://www.adobe.com/support/security/bulletins/apsb09-15.html`

Medium (CVSS: 6.8)
NVT: Adobe Reader Multiple Vulnerabilities - Aug07 (Linux)

Product detection result
cpe:/a:adobe:acrobat_reader:7.0.5
Detected by Adobe products version detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0
↪.800108)

Summary
This host is installed with Adobe Reader and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attacker to conduct denial of service, memory corruption and execution of arbitrary code.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Adobe Reader 8.0 or later. For updates refer to http://get.adobe.com/reader

Affected Software/OS
Adobe Reader before version 8.0 on Linux.

Vulnerability Insight
Flaw exist due to unspecified error within Adobe PDF specification.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Adobe Reader Multiple Vulnerabilities - Aug07 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804266
Version used: $Revision: 2482 $

Product Detection Result
Product: cpe:/a:adobe:acrobat_reader:7.0.5
Method: Adobe products version detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800108)

References
CVE: CVE-2007-0103
BID:21910
Other:
URL:http://xforce.iss.net/xforce/xfdb/31364
URL:http://projects.info-pull.com/moab/MOAB-06-01-2007.html

Medium (CVSS: 5.0)
NVT: Denial Of Service Vulnerability in OpenSSL June-09 (Linux)

Product detection result
cpe:/a:openssl:openssl:0.9.8d
Detected by OpenSSL Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.800335 ↪)

Summary
This host has OpenSSL installed and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attacker to cause DTLS server crash. Impact Level: Application Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSL version 0.9.8i or later http://www.openssl.org/source
*** Note: Vulnerability is related to CVE-2009-1386 *****
**** This might be a False Positive Only version check is being done depending on the publicly available OpenSSL packages. Each vendor might have backported versions of the packages. *****

Affected Software/OS
OpenSSL version prior to 0.9.8i on Linux.

Vulnerability Insight
A NULL pointer dereference error in ssl/s3_pkt.c file which does not properly check the input packets value via a DTLS ChangeCipherSpec packet that occurs before ClientHello.

Vulnerability Detection Method
Details:Denial Of Service Vulnerability in OpenSSL June-09 (Linux)
OID:1.3.6.1.4.1.25623.1.0.800809
Version used: $Revision: 4869 $

Product Detection Result
Product: cpe:/a:openssl:openssl:0.9.8d
Method: OpenSSL Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800335)

References
CVE: CVE-2009-1386
BID:35174
Other:

. . . continues on next page . . .

... continued from previous page ...

URL:http://cvs.openssl.org/chngview?cn=17369
URL:http://www.openwall.com/lists/oss-security/2009/06/02/1
URL:http://rt.openssl.org/Ticket/Display.html?id=1679&user=guest&pass=guest

Medium (CVSS: 4.3)
NVT: Firefox Multiple Vulnerabilities Feb-10 (Linux)

Summary
The host is installed with Firefox Browser and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows attackers to obtain sensitive information via a crafted document.
Impact Level: Application.

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.6, For updates refer to http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Firefox version prior to 3.6 on Linux.

Vulnerability Insight
- The malformed stylesheet document and cross-origin loading of CSS stylesheets even when the stylesheet download has an incorrect MIME type. - IFRAME element allows placing the site&qts URL in the HREF attribute of a stylesheet 'LINK' element, and then reading the 'document.styleSheets[0].href' property value.

Vulnerability Detection Method
Details:Firefox Multiple Vulnerabilities Feb-10 (Linux)
OID:1.3.6.1.4.1.25623.1.0.900743
Version used: $Revision: 5394 $

References
CVE: CVE-2010-0648, CVE-2010-0654
Other:
URL:http://code.google.com/p/chromium/issues/detail?id=9877
URL:http://code.google.com/p/chromium/issues/detail?id=32309

Medium (CVSS: 5.8)
NVT: Firefox URL Spoofing And Phising Vulnerability (Linux)

... continues on next page ...

... continued from previous page ...

Summary
The host is installed with Mozilla Firefox browser and is prone to URL spoofing and phising vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful remote exploitation will let the attacker spoof the URL information by using homoglyphs of say the /(slash) and ?(question mark)and can gain sensitive information by redirecting the user to any malicious URL. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Mozilla Firefox version 3.6.3 or later For updates refer to http://www.mozilla.com/en-US/firefox/

Affected Software/OS
Mozilla Firefox version 3.0.6 and prior on Linux.

Vulnerability Insight
Firefox doesn't properly prevent the literal rendering of homoglyph characters in IDN domain names. This renders the user vulnerable to URL spoofing and phising attacks as the atatcker may redirect the user to a different arbitrary malformed website.

Vulnerability Detection Method
Details:`Firefox URL Spoofing And Phising Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900512
Version used: `$Revision: 5055 $`

References
`CVE: CVE-2009-0652`
`BID:33837`
`Other:`
`URL:http://www.mozilla.org/projects/security/tld-idn-policy-list.html`
`URL:http://www.blackhat.com/html/bh-dc-09/bh-dc-09-speakers.html#Marlinspike`

Medium (CVSS: 6.8)
NVT: GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)

Summary
This host is installed with GZip and is prone to Input Validation Vulnerability

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation could result in Denial of Serivce (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive. Impact Level: Application

Solution
Solution type: VendorFix
Apply the patch or Upgrade to GZip version 1.3.13, http://www.gzip.org/index-f.html#sources
http://git.savannah.gnu.org/cgit/gzip.git/commit/?id=39a362ae9d9b007473381dba5032f4dfc1744cf2
*** NOTE: Ignore this warning, if above mentioned patch is already applied. *****

Affected Software/OS
GZip version prior to 1.3.13 on Linux.

Vulnerability Insight
The flaw is due to error in 'huft_build()' function in 'inflate.c', creates a hufts table that is too small.

Vulnerability Detection Method
Details:`GZip 'huft_build()' in 'inflate.c' Input Validation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800453
Version used: `$Revision: 5306 $`

References
```
CVE: CVE-2009-2624
BID:37888
Other:
  URL:http://secunia.com/advisories/38132
   URL:http://www.vupen.com/english/advisories/2010/0185
   URL:https://bugzilla.redhat.com/show_bug.cgi?id=514711
```

Medium (CVSS: 4.4)
NVT: Insecure Saving Of Downloadable File In Mozilla Firefox (Linux)

Summary
This host is installed with Mozilla Firefox and is prone to insecure saving of downloadable file.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Local attackers may leverage this issue by replacing an arbitrary downloaded file by placing a file in a /tmp location before the download occurs. Impact Level: Application

Solution
Upgrade to Mozilla Firefox version 3.6.3 or later For updates refer to http://www.mozilla.com/en-US/firefox/

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Mozilla Firefox version 2.x, 3.x on Linux.

Vulnerability Insight
This security issue is due to the browser using a fixed path from the /tmp directory when a user opens a file downloaded for opening from the 'Downloads' window. This can be exploited to trick a user into opening a file with potentially malicious content by placing it in the /tmp directory before the download takes place.

Vulnerability Detection Method
Details:`Insecure Saving Of Downloadable File In Mozilla Firefox (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900869
Version used: `$Revision: 5055 $`

References
```
CVE: CVE-2009-3274
Other:
  URL:http://secunia.com/advisories/36649
   URL:http://jbrownsec.blogspot.com/2009/09/vamos-updates.html
   URL:http://securitytube.net/Zero-Day-Demos-%28Firefox-Vulnerability-Discovere
↪d%29-video.aspx
```

Medium (CVSS: 4.3)
NVT: KDE Konqueror Select Object Denial of Service Vulnerability

Summary
This host is installed with KDE Konqueror and is prone to Denial of Service Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will lead to memory consumption and can result in a browser crash.

Solution
Upgrade to KDE Konqueror version 4.4.3 or later. For updates refer to http://www.kde.org/download

Affected Software/OS
KDE Konqueror version 4.2.4 and prior.

Vulnerability Insight
The flaw occurs due to an error while processing Select object whose length property contains a large integer value.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:KDE Konqueror Select Object Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900903
Version used: $Revision: 5055 $

References
CVE: CVE-2009-2537
Other:
URL:http://www.milw0rm.com/exploits/9160
URL:http://www.g-sec.lu/one-bug-to-rule-them-all.html

Medium (CVSS: 5.0)
NVT: Konqueror in KDE Denial of Service Vulnerability

Summary
This host is running Konqueror and is prone to Denial of Service Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attacker to trigger the use of a deleted object within the HTML-Tokenizer::scriptHandler() method and can cause a crash.

Solution
Upgrade to KDE Konqueror version 4.4.3 or later. For updates refer to http://www.kde.org/download

Affected Software/OS
Konqueror in KDE version 3.5.10 or prior.

Vulnerability Insight
These flaws are due to, - improper handling of JavaScript document.load Function calls targeting the current document which can cause denial of service. - HTML parser in KDE Konqueror causes denial of service via a long attribute in HR element or a long BGCOLOR or BORDERCOLOR.

Vulnerability Detection Method
Details:Konqueror in KDE Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900417
Version used: $Revision: 4522 $

References
CVE: CVE-2008-4514, CVE-2008-5712
BID:31696
Other:
URL:http://www.milw0rm.com/exploits/6718
URL:http://secunia.com/advisories/32208

Medium (CVSS: 5.8)
NVT: libcrypt-openssl-dsa-perl Security Bypass Vulnerability in OpenSSL

Summary
This host has OpenSSL installed and is prone to security bypass vulnerability.

Vulnerability Detection Result
`Installed version: 0.9.8d`
`Fixed version: 0.9.8j`

Impact
Successful exploitation will let the attacker spoof the user data with malicious DSA signature to gain access to user's sensitive information. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 0.9.8j http://www.openssl.org/source/

Affected Software/OS
OpenSSL version prior to 0.9.8j on Linux.

Vulnerability Insight
The flaw is due to libcrypt-openssl-dsa-perl which does not properly check the return value from the OpenSSL DSA_verify and DSA_do_verify functions.

Vulnerability Detection Method
Details:`libcrypt-openssl-dsa-perl Security Bypass Vulnerability in OpenSSL`
OID:1.3.6.1.4.1.25623.1.0.800336
Version used: `$Revision: 4918 $`

References
`CVE: CVE-2009-0129, CVE-2008-5077`
`BID:33150`
`Other:`
`URL:http://openwall.com/lists/oss-security/2009/01/12/4`
`URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=511519`

Medium (CVSS: 4.3)
NVT: Mozilla Firefox 'data:' URI XSS Vulnerability - Sep09 (Linux)

Summary
This host is installed with Mozilla Product(s) and is prone to Cross-Site Scripting vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will allow attackers to conduct Cross-Site Scripting attacks in the victim's system. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade Firefox version 3.6.3 or later, For updates refer to http://www.mozilla.org/

Affected Software/OS
Mozilla, Firefox version 3.0.13 and prior, 3.5 and 3.6/3.7 a1 pre on Linux.

Vulnerability Insight
Firefox fails to sanitise the 'data:' URIs in Location headers in HTTP responses, which can be exploited via vectors related to injecting a Location header or Location HTTP response header.

Vulnerability Detection Method
Details:`Mozilla Firefox 'data:' URI XSS Vulnerability - Sep09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800890
Version used: `$Revision: 4865 $`

References
`CVE: CVE-2009-3012`
`Other:`
`URL:http://websecurity.com.ua/3323/`
`URL:http://websecurity.com.ua/3386/`

Medium (CVSS: 4.3)
NVT: Mozilla Firefox 'GIF' File DoS Vulnerability - Nov09 (Linux)

Summary
The host is installed with Firefox browser and is prone to Denial of Service vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allows remote attacker to cause a vulnerable application to crash.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.5.5 or later, http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Mozilla Firefox version prior to 3.5.5 on Linux.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

A NULL pointer dereference error in 'nsGIFDecoder2::GifWrite' function in 'decoders/gif/nsGIFDecoder2.cpp' in libpr0n, which can be exploited to cause application crash via an animated 'GIF' file with a large image size.

Vulnerability Detection Method
Details:`Mozilla Firefox 'GIF' File DoS Vulnerability - Nov09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900895
Version used: `$Revision: 5055 $`

References
`CVE: CVE-2009-3978`
`Other:`
`URL:https://bugzilla.mozilla.org/show_bug.cgi?id=525326`
`URL:https://wiki.mozilla.org/Releases/Firefox_3.5.5/Test_Plan`
`URL:http://hg.mozilla.org/releases/mozilla-1.9.1/rev/edf189567edc`

Medium (CVSS: 5.0)
NVT: Mozilla Firefox 'window.print()' Denial Of Service Vulnerability (Linux)

Summary
This host is installed with Mozilla Firefox and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful attacks may result in Denial of Service condition on the victim's system. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Mozilla Firefox version 3.6.3 or later For updates refer to http://www.mozilla.com/en-US/firefox/

Affected Software/OS
Mozilla Firefox version 3.0.1 and prior on Linux.

Vulnerability Insight
Error exists when application fails to handle user supplied input when calling the 'window.print' function in a loop aka a 'printing DoS attack'.

Vulnerability Detection Method
Details:`Mozilla Firefox 'window.print()' Denial Of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900866
Version used: `$Revision: 5055 $`

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2008-7244
Other:
URL:http://websecurity.com.ua/2456/
URL:http://www.securityfocus.com/archive/1/archive/1/506328/100/100/threaded

Medium (CVSS: 6.8)
NVT: Mozilla Firefox Multiple Vulnerabilities Apr-09 (Linux)

Summary
The host is installed with Mozilla Firefox browser and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could result in Information Disclosure, XSS, Script Injection, Memory Corruption, CSRF, Arbitrary JavaScript code execution or can cause denial of service attacks.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.9 http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Firefox version prior to 3.0.9 on Linux.

Vulnerability Insight
For more information about vulnerabilities on Firefox, go through the links mentioned in references.

Vulnerability Detection Method
Details:Mozilla Firefox Multiple Vulnerabilities Apr-09 (Linux)
OID:1.3.6.1.4.1.25623.1.0.900343
Version used: $Revision: 5055 $

References
CVE: CVE-2009-1302, CVE-2009-1303, CVE-2009-1304, CVE-2009-1305, CVE-2009-1306,
↪CVE-2009-1307, CVE-2009-1308, CVE-2009-1309, CVE-2009-1310, CVE-2009-1311, CVE
↪-2009-1312
BID:34656
Other:
URL:http://secunia.com/advisories/34758
URL:http://www.mozilla.org/security/announce/2009/mfsa2009-14.html
URL:http://www.mozilla.org/security/announce/2009/mfsa2009-16.html
URL:http://www.mozilla.org/security/announce/2009/mfsa2009-17.html

... continues on next page ...

... continued from previous page ...

URL:http://www.mozilla.org/security/announce/2009/mfsa2009-18.html
URL:http://www.mozilla.org/security/announce/2009/mfsa2009-19.html
URL:http://www.mozilla.org/security/announce/2009/mfsa2009-20.html
URL:http://www.mozilla.org/security/announce/2009/mfsa2009-21.html
URL:http://www.mozilla.org/security/announce/2009/mfsa2009-22.html

Medium (CVSS: 5.0)
NVT: Mozilla Firefox SOCKS5 Proxy Server DoS Vulnerability Aug-09 (Linux)

Summary
This host is installed with Mozilla Firefox and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let attacker to cause Denial of Service condition in a affected proxy server. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Firefox version 3.0.12/3.5.2 http://www.mozilla.com/en-US/firefox/all.html

Affected Software/OS
Firefox version before 3.0.12 or 3.5 before 3.5.2 on Linux.

Vulnerability Insight
Error exists when application fails to handle long domain name in a response which leads remote 'SOCKS5' proxy servers into data stream corruption.

Vulnerability Detection Method
Details:Mozilla Firefox SOCKS5 Proxy Server DoS Vulnerability Aug-09 (Linux)
OID:1.3.6.1.4.1.25623.1.0.800858
Version used: $Revision: 4865 $

References
CVE: CVE-2009-2470
BID:35925
Other:
URL:https://bugzilla.mozilla.org/show_bug.cgi?id=459524
URL:http://www.mozilla.org/security/announce/2009/mfsa2009-38.html

Medium (CVSS: 4.3)
NVT: Mozilla Product(s) 'javascript:' URI XSS Vulnerability - Sep09 (Linux)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with Mozilla Product(s) and is prone to Cross-Site Scripting vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to conduct Cross-Site Scripting attacks in the victim's system.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
Mozilla, Firefox version 3.0.13 and prior, 3.5 and 3.6/3.7 a1 pre Moziila Browser 1.7.x and prior. Seamonkey 1.1.17 on Linux.

Vulnerability Insight
Application fails to sanitise the 'javascript:' and 'data:' URIs in Refresh headers or Location headers in HTTP responses, which can be exploited via vectors related to injecting a Refresh header or Location HTTP response header.

Vulnerability Detection Method
Details:`Mozilla Product(s) 'javascript:' URI XSS Vulnerability - Sep09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800886
Version used: `$Revision: 4869 $`

References
```
CVE: CVE-2009-3010, CVE-2009-3014
Other:
  URL:http://websecurity.com.ua/3315/
   URL:http://websecurity.com.ua/3323/
   URL:http://websecurity.com.ua/3373/
   URL:http://websecurity.com.ua/3386/
   URL:http://www.securityfocus.com/archive/1/archive/1/506163/100/0/threaded
```

Medium (CVSS: 6.8)
NVT: Neon Certificate Spoofing and Denial of Service Vulnerability

Summary
This host has Neon installed and is prone to Certificate Spoofing and Denial of Service vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attacker may leverage this issue to conduct man-in-the-middle attacks to spoof arbitrary SSL servers, and can deny the service by memory or CPU consumption on the affected application. Impact Level: System/Application

Solution
Upgrade to version 0.28.6 or latest http://www.webdav.org/neon/

Affected Software/OS
WebDAV, Neon version prior to 0.28.6 on Linux.

Vulnerability Insight
- When OpenSSL is used, neon does not properly handle a '&qt?&qt' character in a domain name in the 'subject&qts' Common Name (CN) field of an X.509 certificate via a crafted certificate issued by a legitimate Certification Authority. - When expat is used, neon does not properly detect recursion during entity expansion via a crafted XML document containing a large number of nested entity references.

Vulnerability Detection Method
Details:`Neon Certificate Spoofing and Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.900828
Version used: `$Revision: 5122 $`

References
```
CVE: CVE-2009-2473, CVE-2009-2474
BID:36080, 36079
Other:
  URL:http://secunia.com/advisories/36371
   URL:http://xforce.iss.net/xforce/xfdb/52633
   URL:http://www.vupen.com/english/advisories/2009/2341
```

Medium (CVSS: 5.0)
NVT: OpenSSL DTLS Packets Multiple Denial of Service Vulnerabilities (Linux)

Product detection result
```
cpe:/a:openssl:openssl:0.9.8d
Detected by OpenSSL Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.800335
↪)
```

Vulnerability Detection Result
`Overview: This host is running OpenSSL and is prone to`

... continues on next page ...

... continued from previous page ...

```
Multiple Denial of Service Vulnerabilities (Linux)
Vulnerability Insight:
 Multiple flaws are due to,
 - The library does not limit the number of buffered DTLS records with a
   future epoch.
 - An error when processing DTLS messages can be exploited to exhaust all
   available memory by sending a large number of out of sequence handshake
   messages.
 Affected Software/OS:
 OpenSSL version 1.0.0 Beta2 and prior on Linux.
Fix: Apply patches or upgrade to the latest version.
For updates refer tohttp://www.openssl.org/source/
References:
http://secunia.com/advisories/35128
http://cvs.openssl.org/chngview?cn=18188
http://www.openwall.com/lists/oss-security/2009/05/18/1
```

Impact
Successful exploitation will allow attacker to cause denial-of-service conditions,crash the client,and exhaust all memory.
Impact Level: System/Application

Solution
Solution type: VendorFix

Vulnerability Detection Method
Details:`OpenSSL DTLS Packets Multiple Denial of Service Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900653
Version used: `$Revision: 3265 $`

Product Detection Result
Product: `cpe:/a:openssl:openssl:0.9.8d`
Method: `OpenSSL Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800335)

References
`CVE: CVE-2009-1377, CVE-2009-1378, CVE-2009-1379`
`BID:35001`

Medium (CVSS: 5.0)
NVT: OpenSSL Multiple Vulnerabilities (Linux)

Summary
This host is installed with OpenSSL and is prone to Multiple Vulnerabilities.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 0.9.8d
Fixed version: 0.9.8k

Impact
Successful exploitation will let the attacker cause memory access violation, security bypass or can cause denial of service.

Solution
Solution type: VendorFix
Upgrade to OpenSSL version 0.9.8k http://openssl.org

Affected Software/OS
OpenSSL version prior to 0.9.8k on all running platform.

Vulnerability Insight
- error exists in the 'ASN1_STRING_print_ex()' function when printing 'BMPString' or 'UniversalString' strings which causes invalid memory access violation. - 'CMS_verify' function incorrectly handles an error condition when processing malformed signed attributes. - error when processing malformed 'ASN1' structures which causes invalid memory access violation.

Vulnerability Detection Method
Details:OpenSSL Multiple Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.800259
Version used: $Revision: 4869 $

References
CVE: CVE-2009-0590, CVE-2009-0591, CVE-2009-0789
BID:34256
Other:
URL:http://secunia.com/advisories/34411
URL:http://www.openssl.org/news/secadv_20090325.txt
URL:http://securitytracker.com/alerts/2009/Mar/1021905.html

Medium (CVSS: 6.8)
NVT: Pango Integer Buffer Overflow Vulnerability

Product detection result
cpe:/a:pango:pango:...
Detected by Pango Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900643)

Summary
This host has installed with Pango and is prone to Integer Buffer Overflow vulnerability

Vulnerability Detection Result
Installed version: ...

... continues on next page ...

... continued from previous page ...

Fixed version: 1.24.0

Impact
Successful exploitation will allow attacker to execute arbitrary code via a long glyph string, and can cause denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to pango version 1.24.0 or later http://ftp.acc.umu.se/pub/GNOME/sources/pango/

Affected Software/OS
Pango version prior to 1.24.0

Vulnerability Insight
Error in pango_glyph_string_set_size function in pango/glyphstring.c file, which fails to perform adequate boundary checks on user-supplied data before using the data to allocate memory buffers.

Vulnerability Detection Method
Details:Pango Integer Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900644
Version used: $Revision: 5122 $

Product Detection Result
Product: cpe:/a:pango:pango:...
Method: Pango Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900643)

References
CVE: CVE-2009-1194
BID:34870
Other:
URL:http://secunia.com/advisories/35018
URL:http://www.debian.org/security/2009/dsa-1798
URL:http://www.openwall.com/lists/oss-security/2009/05/07/1

Medium (CVSS: 5.0)
NVT: PHP 'extract()' Function Security Bypass Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

Summary
This host is running PHP and is prone to security bypass vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.2.15`

Impact
Successful exploitation could allows remote attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input.
Impact Level: Network

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.15 or later For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.2.15

Vulnerability Insight
The flaw is due to error in 'extract()' function, it does not prevent use of the 'EXTR_OVERWRITE' parameter to overwrite the GLOBALS superglobal array.

Vulnerability Detection Method
Details:`PHP 'extract()' Function Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801731
Version used: `$Revision: 4502 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2011-0752`
`Other:`
`URL:http://www.php.net/releases/5_2_15.php`
`URL:http://www.openwall.com/lists/oss-security/2010/12/13/4`

Medium (CVSS: 6.4)
NVT: PHP 'make_http_soap_request' Information Disclosure Vulnerability (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`

... continues on next page ...

... continued from previous page ...

Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to denial of service or information disclosure vulnerabilities

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.4.44

Impact
Successfully exploiting this issue allow remote attackers to obtain sensitive information from process memory or cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or 7.0.4, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 on Linux

Vulnerability Insight
The flaw is due an error in the 'make_http_soap_request' function in 'ext/soap/php_http.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP 'make_http_soap_request' Information Disclosure Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.808666
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-3185
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php

Medium (CVSS: 5.0)
NVT: PHP 'unserialize()' Function Denial of Service Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
The host is running PHP and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: N/A

Impact
Successful exploitation could allow attackers to execute arbitrary PHP code and cause denial of service.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
PHP 5.3.0 and prior on all running platform.

Vulnerability Insight
An error in 'unserialize()' function while processing malformed user supplied data containing a long serialized string passed via the '__wakeup()' or '__destruct()' methods.

Vulnerability Detection Method
Details:PHP 'unserialize()' Function Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900993
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-4418
Other:

... continues on next page ...

... continued from previous page ...

URL:http://www.security-database.com/detail.php?alert=CVE-2009-4418
URL:http://www.suspekt.org/downloads/POC2009-ShockingNewsInPHPExploitation.pd
↪f

Medium (CVSS: 5.0)
NVT: PHP 5.2.8 and Prior Versions Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to multiple security vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.9

Impact
Successful exploits could allow an attacker to cause a denial-of-service condition. An unspecified issue with an unknown impact was also reported.

Solution
Solution type: VendorFix
The vendor has released PHP 5.2.9 to address these issues. Please see http://www.php.net/ fore more information.

Affected Software/OS
These issues affect PHP 5.2.8 and prior versions.

Vulnerability Detection Method
Details:PHP 5.2.8 and Prior Versions Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100146
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-1271
BID:33927

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://www.securityfocus.com/bid/33927
```

Medium (CVSS: 4.3)
NVT: PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)`

Summary
This host is installed with PHP and is prone to cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.4.38`

Impact
Successfully exploiting this issue allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging '%0A%20' or '%0D%0A%20' mishandling in the header function.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.38, or 5.5.22, or 5.6.6, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 on Linux

Vulnerability Insight
The flaw is due to the 'sapi_header_op' function in 'main/SAPI.c' script supports deprecated line folding without considering browser compatibility.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809137
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2015-8935
BID:92356
Other:
URL:https://bugs.php.net/bug.php?id=68978

Medium (CVSS: 6.4)
NVT: PHP dba_replace Denial of Service Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
The host is running PHP and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.7

Impact
Successful exploitation could allow attackers to execute arbitrary code corrupt files and cause denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.7 or later, http://www.php.net/downloads.php

Affected Software/OS
PHP 4.x and 5.2.6 on all running platform.

Vulnerability Insight
An error occurs in 'dba_replace()' function while processing malformed user supplied data containing a key with the NULL byte.

Vulnerability Detection Method
Details:PHP dba_replace Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900925
Version used: $Revision: 4505 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-7068
BID:33498
Other:
URL:http://xforce.iss.net/xforce/xfdb/47316
URL:http://www.securityfocus.com/archive/1/archive/1/498746/100/0/threaded

Medium (CVSS: 6.8)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.18

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.18, or 7.0.3, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.18 and 7.x before 7.0.3 on Linux

Vulnerability Insight
The flaw is due an improper handling of zero-size './/@LongLink' files by 'phar_make_dirstream' function in ext/phar/dirstream.c script.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808609
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-4343
BID:89179
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.openwall.com/lists/oss-security/2016/04/28/2

Medium (CVSS: 6.4)
NVT: PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.31

Impact
Successfully exploiting this issue allow attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 on Linux.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw is due to the 'sapi/fpm/fpm/fpm_log.c' script misinterprets the semantics of the snprintf return value.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.809139
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-5114
BID:81808
Other:
URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 5.0)
NVT: PHP Denial Of Service Vulnerability - April09

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
The host is installed with PHP and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.10

Impact
Successful exploitation could result in denial of service condition.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.9 or above, http://www.php.net/downloads.php

... continues on next page ...

... continued from previous page ...

Workaround: For workaround refer below link, http://cvs.php.net/viewvc.cgi/php-src/ext/json/JSON_parser.c?r1=1.1.2.14&r2=1.1.2.15

Affected Software/OS
PHP version prior to 5.2.9

Vulnerability Insight
Improper handling of .zip file while doing extraction via php_zip_make_relative_path function in php_zip.c file.

Vulnerability Detection Method
Details:`PHP Denial Of Service Vulnerability - April09`
OID:1.3.6.1.4.1.25623.1.0.800393
Version used: `$Revision: 4504 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2009-1272`
`Other:`
`URL:http://www.php.net/releases/5_2_9.php`
`URL:http://www.openwall.com/lists/oss-security/2009/04/01/9`

Medium (CVSS: 5.0)
NVT: PHP FastCGI Module File Extension Denial Of Service Vulnerabilities

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
PHP is prone to a denial-of-service vulnerability because the application fails to handle certain file requests.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 4.4.9`

Impact

... continues on next page ...

... continued from previous page ...

Attackers can exploit this issue to crash the affected application, denying service to legitimate users.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
PHP 4.4 prior to 4.4.9 and PHP 5.2 through 5.2.6 are vulnerable.

Vulnerability Detection Method
Details:PHP FastCGI Module File Extension Denial Of Service Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100582
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-3660
BID:31612
Other:
URL:http://www.securityfocus.com/bid/31612
URL:http://www.openwall.com/lists/oss-security/2008/08/08/2
URL:http://www.php.net/ChangeLog-5.php#5.2.8
URL:http://www.php.net
URL:http://support.avaya.com/elmodocs2/security/ASA-2009-161.htm

Medium (CVSS: 5.0)
NVT: PHP Fileinfo Component Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.0

... continues on next page ...

... continued from previous page ...

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.0 For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.0 on Linux

Vulnerability Insight
The flaw is due an improper validation of input to zero root_storage value in a CDF file.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Fileinfo Component Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808669
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2014-0236`
`BID:90957`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

Medium (CVSS: 5.1)
NVT: PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
This host is installed with PHP and is prone to Man-in-the-middle attack vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 4.4.4
Fixed version: 5.6.24/7.0.9

Impact
Successfully exploiting this issue may allow remote, unauthenticated to conduct MITM attacks on internal server subrequests or direct the server to initiate connections to arbitrary hosts or to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Update to PHP version 5.6.24 or 7.0.19. For updates refer to http://www.php.net

Affected Software/OS
PHP versions 5.x through 5.6.23 and 7.0.x through 7.0.8 on Linux

Vulnerability Insight
The web servers running in a CGI or CGI-like context may assign client request Proxy header values to internal HTTP_PROXY environment variables and 'HTTP_PROXY' is improperly trusted by some PHP libraries and applications and flaw exist in the gdImageCropThreshold function in 'gd_crop.c' in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808628
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-5385, CVE-2016-6128
BID:91821, 91509
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php
URL:http://www.kb.cert.org/vuls/id/797896
URL:https://bugs.php.net/bug.php?id=72573
URL:https://bugs.php.net/bug.php?id=72494

Medium (CVSS: 5.0)
NVT: PHP Multiple Denial of Service Vulnerabilities (Linux)

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.12

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (application crash or memory consuption).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.12 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.12 on Linux

Vulnerability Insight
Multiple flaws are due to - An improper handling of driver behavior for SQL_WVARCHAR columns in the 'odbc_bindcols function' in 'ext/odbc/php_odbc.c' script. - The 'gdImageScaleTwoPass' function in gd_interpolation.c script in the GD Graphics Library uses inconsistent allocate and free approaches.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.808611
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2015-8877, CVE-2015-8879, CVE-2015-8874
BID:90866, 90842, 90714
Other:

... continues on next page ...

... continued from previous page ...

URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 6.8)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed Version: 4.4.4
Fixed Version: 5.5.30

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP 5.5.30 or 5.6.14 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.30 and 5.6.x before 5.6.14

Vulnerability Insight
Multiple flaws are due to, - An Off-by-one error in the 'phar_parse_zipfile' function within ext/phar/zip.c script. - An error in the 'phar_get_entry_data' function in ext/phar/util.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.806649
Version used: $Revision: 5082 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2015-7804, CVE-2015-7803
BID:76959
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:https://bugs.php.net/bug.php?id=70433
URL:http://www.openwall.com/lists/oss-security/2015/10/05/8

Medium (CVSS: 5.0)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.30

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer over-read or application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.30, 7.0.15, 7.1.1 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1.

Vulnerability Insight
Multiple flaws are due to - The exif_convert_any_to_int function in ext/exif/exif.c tries to divide the minimum representable negative integer by -1.
- A mishandled serialized data in a finish_nested_data call within the object_common1 function in ext/standard/var_unserializer.c.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Linux)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.108052
Version used: $Revision: 5099 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-10161, CVE-2016-10158
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/ChangeLog-7.php

Medium (CVSS: 5.0)
NVT: PHP Multiple Security Bypass Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is running PHP and is prone to multiple security bypass vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.4

Impact
Successful exploitation could allow remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact.
Impact Level: Application/Network

Solution
Solution type: VendorFix
Upgrade to PHP 5.3.4 or later For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.3.4

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaws are caused to: - An error in handling pathname which accepts the '?' character in a pathname. - An error in 'iconv_mime_decode_headers()' function in the 'Iconv' extension. - 'SplFileInfo::getType' function in the Standard PHP Library (SPL) extension, does not properly detect symbolic links in windows. - Integer overflow in the 'mt_rand' function. - Race condition in the 'PCNTL extension', when a user-defined signal handler exists.

Vulnerability Detection Method
Details:PHP Multiple Security Bypass Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.801585
Version used: $Revision: 4502 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2006-7243, CVE-2010-4699, CVE-2011-0754, CVE-2011-0753, CVE-2011-0755
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/releases/5_3_4.php
URL:http://openwall.com/lists/oss-security/2010/12/09/9
URL:http://svn.php.net/viewvc?view=revision&revision=305507

Medium (CVSS: 6.4)
NVT: PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to out-of-bounds read memory corruption vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.31

Impact
Successfully exploiting this issue allow remote attackers to obtain sensitive information or cause a denial-of-service condition.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 on Linux

Vulnerability Insight
The flaw is due to memory corruption vulnerability via a large 'bgd_color' argument to the 'imagerotate' function in 'ext/gd/libgd/gd_interpolation.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807504
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-1903`
`BID:79916`
`Other:`
`URL:https://bugs.php.net/bug.php?id=70976`
`URL:http://www.openwall.com/lists/oss-security/2016/01/14/8`

Medium (CVSS: 5.1)
NVT: PHP Ovrimos Extension Code Execution Vulnerability

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
PHP is prone to a code-execution vulnerability due to a design error in a vulnerable extension.

Vulnerability Detection Result
`Installed version: 4.4.4`

... continues on next page ...

... continued from previous page ...

Fixed version: 4.4.5

Impact
Successful exploits may allow an attacker to execute arbitrary code in the context of the affected application. Failed exploits would likely crash PHP.

Solution
Solution type: VendorFix

Affected Software/OS
PHP versions prior to 4.4.5 or 5.2.1 with a compiled 'Ovrimos SQL Server Extension' are vulnerable to this issue.

Vulnerability Insight
For this vulnerability to occur, the non-maintained 'Ovrimos SQL Server Extension' must have been compiled into the targeted PHP implementation.

Vulnerability Detection Method
Details:PHP Ovrimos Extension Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100604
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1379, CVE-2007-1378
BID:22833
Other:
URL:http://www.securityfocus.com/bid/22833
URL:http://www.php.net
URL:http://www.php-security.org/MOPB/MOPB-13-2007.html

Medium (CVSS: 5.0)
NVT: PHP PHP_Binary Heap Information Leak Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary

... continues on next page ...

... continued from previous page ...

PHP 'php_binary' serialization handler is prone to a heap- information leak.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
A local attacker can exploit this issue to obtain sensitive information (such as heap offsets and canaries) that may aid in other attacks.

Solution
Solution type: VendorFix
The vulnerability arises because of a missing boundary check in the extraction of variable names.

Affected Software/OS
PHP4 versions prior to 4.4.5 PHP5 versions prior to 5.2.1

Vulnerability Insight
The vulnerability arises because of a missing boundary check in the extraction of variable names.

Vulnerability Detection Method
Details:PHP PHP_Binary Heap Information Leak Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100603
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1380
BID:22805
Other:
URL:http://www.securityfocus.com/bid/22805
URL:http://www8.itrc.hp.com/service/cki/docDisplay.do?docId=c01056506
URL:http://www.php.net
URL:http://lists.suse.com/archive/suse-security-announce/2007-May/0007.html

Medium (CVSS: 6.8)
NVT: PHP Printf() Function 64bit Casting Multiple Format String Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103

... continues on next page ...

... continued from previous page ...

↪592)

Summary
PHP is prone to multiple format-string vulnerabilities due to a design error when casting 64-bit variables to 32 bits.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
Attackers may be able to exploit these issues to execute arbitrary code in the context of the webserver process or to cause denial-of-service conditions.

Solution
Solution type: VendorFix
The vendor released versions 5.2.1 and 4.4.5 to address these issues. Please see the references for more information.

Affected Software/OS
These issues affect PHP versions prior to 4.4.5 and 5.2.1 running on 64-bit computers.

Vulnerability Detection Method
Details:PHP Printf() Function 64bit Casting Multiple Format String Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100595
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1884
BID:23219
Other:
URL:http://www.securityfocus.com/bid/23219
URL:http://www8.itrc.hp.com/service/cki/docDisplay.do?docId=c01056506
URL:http://www.php-security.org/MOPB/MOPB-38-2007.html
URL:http://www.php.net/releases/4_4_5.php
URL:http://www.php.net/releases/5_2_1.php
URL:http://www.php.net

Medium (CVSS: 4.3)
NVT: PHP SOAP Parser Multiple Information Disclosure Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple information disclosure vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.22/5.4.12

Impact
Successful exploitation will allow remote attackers to obtain sensitive information.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP 5.3.22 or 5.4.12 or later, http://www.php.net/downloads.php

Affected Software/OS
PHP version before 5.3.22 and 5.4.x before 5.4.12

Vulnerability Insight
Flaws are due to the way SOAP parser process certain SOAP objects (due to allowed expansion of XML external entities during SOAP WSDL files parsing).

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:PHP SOAP Parser Multiple Information Disclosure Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.803764
Version used: $Revision: 5351 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2013-1824
BID:62373
Other:

... continues on next page ...

... continued from previous page ...

URL:http://php.net/ChangeLog-5.php
URL:http://git.php.net/?p=php-src.git;a=commit;h=afe98b7829d50806559acac9b530
↪acb8283c3bf4

Medium (CVSS: 5.0)
NVT: PHP Version < 5.1.0 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.1.0 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.1.0

Solution
Solution type: VendorFix
Update PHP to version 5.1.0 or later.

Vulnerability Detection Method
Details:PHP Version < 5.1.0 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110170
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2005-3319, CVE-2005-3883
BID:15177, 15571

Medium (CVSS: 6.8)
NVT: PHP Version < 5.2.3 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103

... continues on next page ...

... continued from previous page ...

↪592)

Summary
PHP version smaller than 5.2.3 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.3

Solution
Solution type: VendorFix
Update PHP to version 5.2.3 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.3 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110189
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1900, CVE-2007-2756, CVE-2007-2872, CVE-2007-3007
BID:23359, 24089, 24259, 24261

Medium (CVSS: 5.0)
NVT: PHP Version < 5.2.9 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.9 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.9

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update PHP to version 5.2.9 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.9 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110187
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-5498, CVE-2009-1271, CVE-2009-1272
BID:33002, 33927

Medium (CVSS: 6.8)
NVT: PHP Version < 5.3.4 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.3.4 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.4

Solution
Solution type: VendorFix
Update PHP to version 5.3.4 or later.

Vulnerability Detection Method
Details:PHP Version < 5.3.4 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110181
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.103592)

References

```
CVE: CVE-2006-7243, CVE-2010-2094, CVE-2010-2950, CVE-2010-3436, CVE-2010-3709,
↪CVE-2010-3710, CVE-2010-3870, CVE-2010-4150, CVE-2010-4156, CVE-2010-4409, CVE
↪-2010-4697, CVE-2010-4698, CVE-2010-4699, CVE-2010-4700, CVE-2011-0753, CVE-20
↪11-0754, CVE-2011-0755
BID:40173, 43926, 44605, 44718, 44723, 44951, 44980, 45119, 45335, 45338, 45339,
↪ 45952, 45954, 46056, 46168
```

Medium (CVSS: 6.4)
NVT: PHP Version < 5.3.9 Multiple Vulnerabilities

Product detection result

```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary

PHP version < 5.3.9 suffers from multiple vulnerabilities such as DOS by sending crafted requests including hash collision parameter values. Several errors exist in some certain functions as well.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     5.3.9
```

Solution

Solution type: VendorFix

Upgrade PHP to 5.3.9 or versions after.

Vulnerability Detection Method

Details:`PHP Version < 5.3.9 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.110012
Version used: `$Revision: 4589 $`

Product Detection Result

Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References

```
CVE: CVE-2011-4566, CVE-2011-4885, CVE-2012-0057, CVE-2012-0781, CVE-2012-0788,
↪CVE-2012-0789
BID:50907, 51193, 51806, 51952, 51992, 52043
```

Medium (CVSS: 6.8)
NVT: PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to XML entity expansion and XML external entity vulnerbilities

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.22

Impact
Successfully exploiting this issue allow remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.22, or 5.6.6, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.22 and 5.6.x before 5.6.6 on Linux

Vulnerability Insight
The flaw is due to script 'ext/libxml/libxml.c' does not isolate each thread from 'libxml_disable_entity_loader' when PHP-FPM is used.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.808615
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2015-8866
BID:87470

. . . continues on next page . . .

... continued from previous page ...

Other:
URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 6.8)
NVT: PHP Zend and GD Multiple Denial of Service Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is running PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.15/5.3.5

Impact
Successful exploitation could allow local attackers to crash the affected application, denying service to legitimate users.
Impact Level: Application/Network

Solution
Solution type: VendorFix
Upgrade to PHP 5.3.5 or later For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.2.15 and 5.3.x before 5.3.4

Vulnerability Insight
The flaws are due to: - An use-after-free error in the 'Zend' engine, which allows remote attackers to cause a denial of service. - A stack-based buffer overflow in the 'GD' extension, which allows attackers to cause a denial of service.

Vulnerability Detection Method
Details:PHP Zend and GD Multiple Denial of Service Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.801586
Version used: $Revision: 4502 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2010-4697, CVE-2010-4698
Other:
URL:http://bugs.php.net/52879
URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 4.0)
NVT: ProFTPD Denial of Service Vulnerability

Product detection result
cpe:/a:proftpd:proftpd:1.3.0
Detected by ProFTPD Server Version Detection (Local) (OID: 1.3.6.1.4.1.25623.1.0
↪.900506)

Summary
The host is running ProFTPD and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 1.3.0
Fixed version: 1.3.2rc3

Impact
Successful exploitation will allow attackers to cause a denial of service. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to ProFTPD version 1.3.2rc3 or later, For updates refer to http://www.proftpd.org/

Affected Software/OS
ProFTPD versions prior to 1.3.2rc3

Vulnerability Insight
The flaw is due to an error in 'pr_data_xfer()' function which allows remote authenticated users to cause a denial of service (CPU consumption) via an ABOR command during a data transfer.

Vulnerability Detection Method
Details:ProFTPD Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801640
Version used: $Revision: 4774 $

Product Detection Result
Product: cpe:/a:proftpd:proftpd:1.3.0
Method: ProFTPD Server Version Detection (Local)
OID: 1.3.6.1.4.1.25623.1.0.900506)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2008-7265
Other:
URL:http://bugs.proftpd.org/show_bug.cgi?id=3131

Medium (CVSS: 6.8)
NVT: ProFTPD Long Command Handling Security Vulnerability

Product detection result
cpe:/a:proftpd:proftpd:1.3.0
Detected by ProFTPD Server Version Detection (Local) (OID: 1.3.6.1.4.1.25623.1.0
↪.900506)

Summary
The host is running ProFTPD Server, which is prone to cross-site request forgery vulnerability.

Vulnerability Detection Result
Installed version: 1.3.0
Fixed version: 1.3.2rc3

Impact
This can be exploited to execute arbitrary FTP commands on another user's session privileges.
Impact Level : Application

Solution
Solution type: VendorFix
Upgrade to the latest version 1.3.2rc3, http://www.proftpd.org/

Affected Software/OS
ProFTPD Server version prior 1.3.2rc3

Vulnerability Insight
The flaw exists due to the application truncating an overly long FTP command, and improperly interpreting the remainder string as a new FTP command.

Vulnerability Detection Method
Details:ProFTPD Long Command Handling Security Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900133
Version used: $Revision: 4774 $

Product Detection Result
Product: cpe:/a:proftpd:proftpd:1.3.0
Method: ProFTPD Server Version Detection (Local)
OID: 1.3.6.1.4.1.25623.1.0.900506)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2008-4242
BID:31289
Other:
URL:http://secunia.com/advisories/31930/
URL:http://bugs.proftpd.org/show_bug.cgi?id=3115

Medium (CVSS: 5.8)
NVT: ProFTPD mod_tls Module NULL Character CA SSL Certificate Validation Security Bypass Vulnerability

Product detection result
cpe:/a:proftpd:proftpd:1.3.0
Detected by ProFTPD Server Version Detection (Local) (OID: 1.3.6.1.4.1.25623.1.0
↪.900506)

Summary
ProFTPD is prone to a security-bypass vulnerability because the application fails to properly validate the domain name in a signed CA certificate, allowing attackers to substitute malicious SSL certificates for trusted ones.

Vulnerability Detection Result
Installed version: 1.3.0
Fixed version: 1.3.2b/1.3.3rc2

Impact
Successful exploits allows attackers to perform man-in-the- middle attacks or impersonate trusted servers, which will aid in further attacks.

Solution
Solution type: VendorFix
Updates are available. Please see the references for details.

Affected Software/OS
Versions prior to ProFTPD 1.3.2b and 1.3.3 to 1.3.3.rc1 are vulnerable.

Vulnerability Detection Method
Details:ProFTPD mod_tls Module NULL Character CA SSL Certificate Validation Security By.
↪..
OID:1.3.6.1.4.1.25623.1.0.100316
Version used: $Revision: 4774 $

Product Detection Result
Product: cpe:/a:proftpd:proftpd:1.3.0

... continues on next page ...

... continued from previous page ...

Method: ProFTPD Server Version Detection (Local)
OID: 1.3.6.1.4.1.25623.1.0.900506)

References
CVE: CVE-2009-3639
BID:36804
Other:
URL:http://www.securityfocus.com/bid/36804
URL:http://bugs.proftpd.org/show_bug.cgi?id=3275
URL:http://www.proftpd.org

Medium (CVSS: 5.1)
NVT: Replay Attack Vulnerability in Tor (Linux)

Summary
This host is installed with Tor Anonymity Proxy and is prone to replay attack vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let the remote attacker cause replay attacks in the network and can compromise router functionalities.
Impact level: Network

Solution
Solution type: VendorFix
Upgrade to Tor version 0.2.1.25 or later, For updates refer to https://www.torproject.org/download-unix.html.en

Affected Software/OS
Tor version 0.2.0.34 and prior on Linux.

Vulnerability Insight
Flaw is in the data flow at the end of the circuit which lets the attacker to modify the relayed data.

Vulnerability Detection Method
Details:Replay Attack Vulnerability in Tor (Linux)
OID:1.3.6.1.4.1.25623.1.0.900323
Version used: $Revision: 5148 $

References
CVE: CVE-2009-0654
Other:

... continues on next page ...

... continued from previous page ...

URL:http://blog.torproject.org/blog/one-cell-enough
URL:http://www.blackhat.com/presentations/bh-dc-09/Fu/BlackHat-DC-09-Fu-Break-Tors-Anonymity.pdf

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2006-298-01 qt

Summary
The remote host is missing an update as announced via advisory SSA:2006-298-01.

Vulnerability Detection Result
Package qt-3.3.6-i486-1 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-298-01

Vulnerability Insight
New qt packages are available for Slackware 10.0, 10.1, 10.2, and 11.0 to fix a possible security issue.
Trolltech has put out a press release which may be found here:
http://www.trolltech.com/company/newsroom/announcements/press.2006-10-19.5434451733

Vulnerability Detection Method
Details:Slackware Advisory SSA:2006-298-01 qt
OID:1.3.6.1.4.1.25623.1.0.57697
Version used: $Revision: 5888 $

References
CVE: CVE-2006-4811

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2006-298-01 qt

Summary
The remote host is missing an update as announced via advisory SSA:2006-298-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-298-01

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

New qt packages are available for Slackware 10.0, 10.1, 10.2, and 11.0 to fix a possible security issue.
Trolltech has put out a press release which may be found here:
http://www.trolltech.com/company/newsroom/announcements/press.2006-10-19.5434451733

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-298-01 qt`
OID:1.3.6.1.4.1.25623.1.0.57697
Version used: `$Revision: 5888 $`

References
`CVE: CVE-2006-4811`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2006-310-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2006-310-01.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-310-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix security issues. The minimum OpenSSL version was raised to OpenSSL 0.9.7l and OpenSSL 0.9.8d to avoid exposure to known security flaws in older versions (these patches were already issued for Slackware). If you have not upgraded yet, get those as well to prevent a potentially exploitable security problem in named.
In addition, the default RSA exponent was changed from 3 to 65537.
Both of these issues are essentially the same as ones discovered in OpenSSL at the end of September 2006, only now there's protection against compiling using the wrong OpenSSL version. RSA keys using exponent 3 (which was previously BIND's default) will need to be regenerated to protect against the forging of RRSIGs.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-310-01 bind`
OID:1.3.6.1.4.1.25623.1.0.57698
Version used: `$Revision: 5963 $`

References
`CVE: CVE-2006-4339`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2006-310-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2006-310-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-310-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix security issues. The minimum OpenSSL version was raised to OpenSSL 0.9.7l and OpenSSL 0.9.8d to avoid exposure to known security flaws in older versions (these patches were already issued for Slackware). If you have not upgraded yet, get those as well to prevent a potentially exploitable security problem in named.
In addition, the default RSA exponent was changed from 3 to 65537.
Both of these issues are essentially the same as ones discovered in OpenSSL at the end of September 2006, only now there's protection against compiling using the wrong OpenSSL version. RSA keys using exponent 3 (which was previously BIND's default) will need to be regenerated to protect against the forging of RRSIGs.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-310-01 bind`
OID:1.3.6.1.4.1.25623.1.0.57698
Version used: `$Revision: 5963 $`

References
`CVE: CVE-2006-4339`

Medium (CVSS: 4.0)
NVT: Slackware Advisory SSA:2006-335-01 tar

Summary
The remote host is missing an update as announced via advisory SSA:2006-335-01.

Vulnerability Detection Result
`Package tar-1.15.1-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-335-01

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

New tar packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-335-01 tar`
OID:1.3.6.1.4.1.25623.1.0.57704
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2006-6097`

Medium (CVSS: 4.0)
NVT: Slackware Advisory SSA:2006-335-01 tar

Summary
The remote host is missing an update as announced via advisory SSA:2006-335-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-335-01

Vulnerability Insight
New tar packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-335-01 tar`
OID:1.3.6.1.4.1.25623.1.0.57704
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2006-6097`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2007-093-03 qt

Summary
The remote host is missing an update as announced via advisory SSA:2007-093-03.

Vulnerability Detection Result
`Package qt-3.3.6-i486-1 is installed which is known to be vulnerable.`

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-093-03

Vulnerability Insight
New qt packages are available for Slackware 10.2, 11.0, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-093-03 qt`
OID:1.3.6.1.4.1.25623.1.0.58197
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2007-0242`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2007-093-03 qt

Summary
The remote host is missing an update as announced via advisory SSA:2007-093-03.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-093-03

Vulnerability Insight
New qt packages are available for Slackware 10.2, 11.0, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-093-03 qt`
OID:1.3.6.1.4.1.25623.1.0.58197
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2007-0242`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2007-110-01 Slackware 11.0 x11-6.9.0 patch fix

Summary
The remote host is missing an update as announced via advisory SSA:2007-110-01.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`Package x11-6.9.0-i486-11 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-110-01

Vulnerability Insight
A new x11-6.9.0-i486-14_slack11.0.tgz patch is available for Slackware 11.0 to fix the inadvertent inclusion of two old fontconfig binaries. Installing the original fontconfig patch followed by the original x11 patch would cause fc-cache and fc-list to be overwritten by old versions, breaking fontconfig.
To fix the issue, reinstall the fontconfig patch. The x11 package has been updated so that installation will not be order-specific for anyone fetching the patches now.
Sorry for the inconvenience.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-110-01 Slackware 11.0 x11-6.9.0 patch fix`
OID:1.3.6.1.4.1.25623.1.0.58228
Version used: `$Revision: 5977 $`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2007-110-01 Slackware 11.0 x11-6.9.0 patch fix

Summary
The remote host is missing an update as announced via advisory SSA:2007-110-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-110-01

Vulnerability Insight
A new x11-6.9.0-i486-14_slack11.0.tgz patch is available for Slackware 11.0 to fix the inadvertent inclusion of two old fontconfig binaries. Installing the original fontconfig patch followed by the original x11 patch would cause fc-cache and fc-list to be overwritten by old versions, breaking fontconfig.
To fix the issue, reinstall the fontconfig patch. The x11 package has been updated so that installation will not be order-specific for anyone fetching the patches now.
Sorry for the inconvenience.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-110-01 Slackware 11.0 x11-6.9.0 patch fix`
OID:1.3.6.1.4.1.25623.1.0.58228
Version used: `$Revision: 5977 $`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2007-136-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2007-136-01.

Vulnerability Detection Result
`Package libpng-1.2.12-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-136-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-136-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.58281
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2007-2445`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2007-136-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2007-136-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-136-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-136-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.58281
Version used: `$Revision: 5912 $`

. . . continues on next page . . .

. . . continued from previous page . . .

References
CVE: CVE-2007-2445

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2007-164-01 libexif

Summary
The remote host is missing an update as announced via advisory SSA:2007-164-01.

Vulnerability Detection Result
Package libexif-0.6.13-i486-2 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-164-01

Vulnerability Insight
New libexif packages are available for Slackware 10.2, 11.0, and -current to fix a crash and potential security issue.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2007-164-01 libexif
OID:1.3.6.1.4.1.25623.1.0.58553
Version used: $Revision: 5912 $

References
CVE: CVE-2007-4168

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2007-164-01 libexif

Summary
The remote host is missing an update as announced via advisory SSA:2007-164-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-164-01

Vulnerability Insight
New libexif packages are available for Slackware 10.2, 11.0, and -current to fix a crash and potential security issue.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-164-01 libexif`
OID:1.3.6.1.4.1.25623.1.0.58553
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2007-4168`

Medium (CVSS: 5.1)
NVT: Slackware Advisory SSA:2007-178-01 gd

Summary
The remote host is missing an update as announced via advisory SSA:2007-178-01.

Vulnerability Detection Result
`Package gd-2.0.33-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-178-01

Vulnerability Insight
GD is an open source code library for the dynamic creation of images.
New gd packages are available for Slackware 11.0, and -current to fix possible security issues.
Please see: http://www.libgd.org/ReleaseNote020035 for complete release notes. 'Upgrading is strongly recommended.'

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-178-01 gd`
OID:1.3.6.1.4.1.25623.1.0.58552
Version used: `$Revision: 6022 $`

Medium (CVSS: 5.1)
NVT: Slackware Advisory SSA:2007-178-01 gd

Summary
The remote host is missing an update as announced via advisory SSA:2007-178-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-178-01

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
GD is an open source code library for the dynamic creation of images.
New gd packages are available for Slackware 11.0, and -current to fix possible security issues.
Please see: http://www.libgd.org/ReleaseNote020035 for complete release notes. 'Upgrading is strongly recommended.'

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-178-01 gd`
OID:1.3.6.1.4.1.25623.1.0.58552
Version used: `$Revision: 6022 $`

Medium (CVSS: 5.8)
NVT: Slackware Advisory SSA:2007-207-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2007-207-01.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-207-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 to fix security issues.
The first issue which allows remote attackers to make recursive queries only affects Slackware 12.0.
The second issue is the discovery that BIND9's query IDs are cryptographically weak. This issue affects the versions of BIND9 in all supported Slackware versions.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-207-01 bind`
OID:1.3.6.1.4.1.25623.1.0.59008
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2007-2925, CVE-2007-2926`

Medium (CVSS: 5.8)
NVT: Slackware Advisory SSA:2007-207-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2007-207-01.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-207-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 to fix security issues.
The first issue which allows remote attackers to make recursive queries only affects Slackware 12.0.
The second issue is the discovery that BIND9's query IDs are cryptographically weak. This issue affects the versions of BIND9 in all supported Slackware versions.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-207-01 bind`
OID:1.3.6.1.4.1.25623.1.0.59008
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2007-2925, CVE-2007-2926`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-222-01 gimp

Summary
The remote host is missing an update as announced via advisory SSA:2007-222-01.

Vulnerability Detection Result
`Package gimp-2.2.13-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-222-01

Vulnerability Insight
New gimp packages are available for Slackware 10.2, 11.0, and 12.0 to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-222-01 gimp`
OID:1.3.6.1.4.1.25623.1.0.59005
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2007-2949`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-222-01 gimp

Summary
The remote host is missing an update as announced via advisory SSA:2007-222-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-222-01

Vulnerability Insight
New gimp packages are available for Slackware 10.2, 11.0, and 12.0 to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-222-01 gimp`
OID:1.3.6.1.4.1.25623.1.0.59005
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2007-2949`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-222-03 qt

Summary
The remote host is missing an update as announced via advisory SSA:2007-222-03.

Vulnerability Detection Result
`Package qt-3.3.6-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-222-03

Vulnerability Insight
New qt packages are available for Slackware 10.2, 11.0, and 12.0 to fix format string errors.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-222-03 qt`
OID:1.3.6.1.4.1.25623.1.0.59003
Version used: `$Revision: 5958 $`

References
`CVE: CVE-2007-3388`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-222-03 qt

Summary
The remote host is missing an update as announced via advisory SSA:2007-222-03.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-222-03

Vulnerability Insight
New qt packages are available for Slackware 10.2, 11.0, and 12.0 to fix format string errors.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-222-03 qt`
OID:1.3.6.1.4.1.25623.1.0.59003
Version used: `$Revision: 5958 $`

References
`CVE: CVE-2007-3388`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-222-05 xpdf

Summary
The remote host is missing an update as announced via advisory SSA:2007-222-05.

Vulnerability Detection Result
`Package xpdf-3.01-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-222-05

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 to fix an integer overflow.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-222-05 xpdf`
OID:1.3.6.1.4.1.25623.1.0.59001
Version used: `$Revision: 5888 $`

References

. . . continues on next page . . .

. . . continued from previous page . . .

CVE: CVE-2007-3387

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-222-05 xpdf

Summary
The remote host is missing an update as announced via advisory SSA:2007-222-05.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-222-05

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 to fix an integer overflow.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2007-222-05 xpdf
OID:1.3.6.1.4.1.25623.1.0.59001
Version used: $Revision: 5888 $

References
CVE: CVE-2007-3387

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-230-01 tcpdump

Summary
The remote host is missing an update as announced via advisory SSA:2007-230-01.

Vulnerability Detection Result
Package tcpdump-3.9.4-i486-2 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-230-01

Vulnerability Insight
New tcpdump packages are available for Slackware 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 to fix a security issue.

Vulnerability Detection Method

. . . continues on next page . . .

... continued from previous page ...

Details:Slackware Advisory SSA:2007-230-01 tcpdump
OID:1.3.6.1.4.1.25623.1.0.59000
Version used: $Revision: 5912 $

References
CVE: CVE-2007-3798

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-230-01 tcpdump

Summary
The remote host is missing an update as announced via advisory SSA:2007-230-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-230-01

Vulnerability Insight
New tcpdump packages are available for Slackware 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 to fix a security issue.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2007-230-01 tcpdump
OID:1.3.6.1.4.1.25623.1.0.59000
Version used: $Revision: 5912 $

References
CVE: CVE-2007-3798

Medium (CVSS: 6.9)
NVT: Slackware Advisory SSA:2007-255-02 samba

Summary
The remote host is missing an update as announced via advisory SSA:2007-255-02.

Vulnerability Detection Result
Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-255-02

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, and 12.0 to fix a security issue and various other bugs.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-255-02 samba`
OID:1.3.6.1.4.1.25623.1.0.59013
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2007-4138`

Medium (CVSS: 6.9)
NVT: Slackware Advisory SSA:2007-255-02 samba

Summary
The remote host is missing an update as announced via advisory SSA:2007-255-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-255-02

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, and 12.0 to fix a security issue and various other bugs.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-255-02 samba`
OID:1.3.6.1.4.1.25623.1.0.59013
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2007-4138`

Medium (CVSS: 6.5)
NVT: Slackware Advisory SSA:2007-283-01 glibc-zoneinfo

Summary
The remote host is missing an update as announced via advisory SSA:2007-283-01.

Vulnerability Detection Result
`Package glibc-zoneinfo-2.3.6-noarch-6 is installed which is known to be vulnerab`

... continues on next page ...

... continued from previous page ...

↪le.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-283-01

Vulnerability Insight
New glibc-zoneinfo packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 to update the timezone tables to the latest versions. If you've noticed your clock has wandered off, these packages should fix the problem.
This isn't really a 'security issue' (or is a minor one), but it's an important fix nevertheless.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-283-01 glibc-zoneinfo`
OID:1.3.6.1.4.1.25623.1.0.59017
Version used: `$Revision: 5950 $`

Medium (CVSS: 6.5)
NVT: Slackware Advisory SSA:2007-283-01 glibc-zoneinfo

Summary
The remote host is missing an update as announced via advisory SSA:2007-283-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-283-01

Vulnerability Insight
New glibc-zoneinfo packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, and 12.0 to update the timezone tables to the latest versions. If you've noticed your clock has wandered off, these packages should fix the problem.
This isn't really a 'security issue' (or is a minor one), but it's an important fix nevertheless.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-283-01 glibc-zoneinfo`
OID:1.3.6.1.4.1.25623.1.0.59017
Version used: `$Revision: 5950 $`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2007-325-01 libpng

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update as announced via advisory SSA:2007-325-01.

Vulnerability Detection Result
`Package libpng-1.2.12-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-325-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-325-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.59024
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2007-5266, CVE-2007-5267, CVE-2007-5268, CVE-2007-5269`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2007-325-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2007-325-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-325-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-325-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.59024
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2007-5266, CVE-2007-5267, CVE-2007-5268, CVE-2007-5269`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-335-01 rsync

Summary
The remote host is missing an update as announced via advisory SSA:2007-335-01.

Vulnerability Detection Result
`Package rsync-2.6.8-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-335-01

Vulnerability Insight
New rsync packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-335-01 rsync`
OID:1.3.6.1.4.1.25623.1.0.59923
Version used: `$Revision: 6018 $`

References
`CVE: CVE-2007-4091`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-335-01 rsync

Summary
The remote host is missing an update as announced via advisory SSA:2007-335-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-335-01

Vulnerability Insight
New rsync packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2007-335-01 rsync`
OID:1.3.6.1.4.1.25623.1.0.59923
Version used: `$Revision: 6018 $`

. . . continues on next page . . .

... continued from previous page ...

References
CVE: CVE-2007-4091

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-337-01 cairo

Summary
The remote host is missing an update as announced via advisory SSA:2007-337-01.

Vulnerability Detection Result
Package cairo-1.0.4-i486-1 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-337-01

Vulnerability Insight
New cairo packages are available for Slackware 11.0, 12.0, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2007-337-01 cairo
OID:1.3.6.1.4.1.25623.1.0.59922
Version used: $Revision: 5950 $

References
CVE: CVE-2007-5503

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2007-337-01 cairo

Summary
The remote host is missing an update as announced via advisory SSA:2007-337-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2007-337-01

Vulnerability Insight
New cairo packages are available for Slackware 11.0, 12.0, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2007-337-01 cairo

... continues on next page ...

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.59922
Version used: `$Revision: 5950 $`

References
`CVE: CVE-2007-5503`

Medium (CVSS: 6.9)
NVT: Slackware Advisory SSA:2008-095-01 openssh

Summary
The remote host is missing an update as announced via advisory SSA:2008-095-01.

Vulnerability Detection Result
`Package openssh-4.4p1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-095-01

Vulnerability Insight
New openssh packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-095-01 openssh`
OID:1.3.6.1.4.1.25623.1.0.60667
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2008-1483`

Medium (CVSS: 6.9)
NVT: Slackware Advisory SSA:2008-095-01 openssh

Summary
The remote host is missing an update as announced via advisory SSA:2008-095-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-095-01

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

New openssh packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-095-01 openssh`
OID:1.3.6.1.4.1.25623.1.0.60667
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2008-1483`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2008-098-02 bzip2

Summary
The remote host is missing an update as announced via advisory SSA:2008-098-02.

Vulnerability Detection Result
`Package bzip2-1.0.3-i486-3 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-098-02

Vulnerability Insight
New bzip2 packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix a DoS issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-098-02 bzip2`
OID:1.3.6.1.4.1.25623.1.0.60826
Version used: `$Revision: 5977 $`

References
`CVE: CVE-2008-1372`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2008-098-02 bzip2

Summary
The remote host is missing an update as announced via advisory SSA:2008-098-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-098-02

Vulnerability Insight
New bzip2 packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, and -current to fix a DoS issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-098-02 bzip2`
OID:1.3.6.1.4.1.25623.1.0.60826
Version used: `$Revision: 5977 $`

References
`CVE: CVE-2008-1372`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2008-191-02 bind

Summary
The remote host is missing an update as announced via advisory SSA:2008-191-02.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-191-02

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, and -current to address a security problem.
More details may be found at the following links:
http://www.isc.org/sw/bind/bind-security.php http://www.kb.cert.org/vuls/id/800113

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-191-02 bind`
OID:1.3.6.1.4.1.25623.1.0.61464
Version used: `$Revision: 6018 $`

References
`CVE: CVE-2008-1447`

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2008-191-02 bind

Summary
The remote host is missing an update as announced via advisory SSA:2008-191-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-191-02

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, and -current to address a security problem.
More details may be found at the following links:
http://www.isc.org/sw/bind/bind-security.php http://www.kb.cert.org/vuls/id/800113

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-191-02 bind`
OID:1.3.6.1.4.1.25623.1.0.61464
Version used: `$Revision: 6018 $`

References
`CVE: CVE-2008-1447`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2008-210-08 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2008-210-08.

Vulnerability Detection Result
`Package openssl-solibs-0.9.8d-i486-1 is installed which is known to be vulnerabl`
`↪e.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-210-08

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, and -current to fix security issues.

... continues on next page ...

... continued from previous page ...

Upgraded OpenSSH packages have been provided to make sure that ssh is not broken my the update – especially if your machine is a remote one, be SURE to upgrade to the new openssh package as well!

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-210-08 openssl`
OID:1.3.6.1.4.1.25623.1.0.61470
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2008-0891, CVE-2008-1672`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2008-210-08 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2008-210-08.

Vulnerability Detection Result
`Package openssl-0.9.8d-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-210-08

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, and -current to fix security issues.
Upgraded OpenSSH packages have been provided to make sure that ssh is not broken my the update – especially if your machine is a remote one, be SURE to upgrade to the new openssh package as well!

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-210-08 openssl`
OID:1.3.6.1.4.1.25623.1.0.61470
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2008-0891, CVE-2008-1672`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2008-210-08 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2008-210-08.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`Package openssh-4.4p1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-210-08

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, and -current to fix security issues.
Upgraded OpenSSH packages have been provided to make sure that ssh is not broken my the update – especially if your machine is a remote one, be SURE to upgrade to the new openssh package as well!

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-210-08 openssl`
OID:1.3.6.1.4.1.25623.1.0.61470
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2008-0891, CVE-2008-1672`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2008-210-08 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2008-210-08.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-210-08

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, and -current to fix security issues.
Upgraded OpenSSH packages have been provided to make sure that ssh is not broken my the update – especially if your machine is a remote one, be SURE to upgrade to the new openssh package as well!

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-210-08 openssl`
OID:1.3.6.1.4.1.25623.1.0.61470

... continues on next page ...

. . . continued from previous page . . .

Version used: `$Revision: 6022 $`

References
`CVE: CVE-2008-0891, CVE-2008-1672`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2008-334-01 ruby

Summary
The remote host is missing an update as announced via advisory SSA:2008-334-01.

Vulnerability Detection Result
`Package ruby-1.8.4-i686-1kjz is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-334-01

Vulnerability Insight
New ruby packages are available for Slackware 11.0, 12.0, and 12.1 to fix bugs and a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-334-01 ruby`
OID:1.3.6.1.4.1.25623.1.0.61947
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2008-1447`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2008-334-01 ruby

Summary
The remote host is missing an update as announced via advisory SSA:2008-334-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2008-334-01

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

New ruby packages are available for Slackware 11.0, 12.0, and 12.1 to fix bugs and a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2008-334-01 ruby`
OID:1.3.6.1.4.1.25623.1.0.61947
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2008-1447`

Medium (CVSS: 5.8)
NVT: Slackware Advisory SSA:2009-014-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2009-014-01.

Vulnerability Detection Result
`Package openssl-0.9.8d-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-014-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue when connecting to an SSL/TLS server that uses a certificate containing a DSA or ECDSA key.
More details about this issue may be found here: http://www.openssl.org/news/secadv_20090107.txt
http://www.ocert.org/advisories/ocert-2008-016.html

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-014-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.63232
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2008-5077`

Medium (CVSS: 5.8)
NVT: Slackware Advisory SSA:2009-014-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2009-014-01.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`Package openssl-solibs-0.9.8d-i486-1 is installed which is known to be vulnerabl`
`↪e.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-014-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue when connecting to an SSL/TLS server that uses a certificate containing a DSA or ECDSA key.
More details about this issue may be found here: http://www.openssl.org/news/secadv_20090107.txt
http://www.ocert.org/advisories/ocert-2008-016.html

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-014-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.63232
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2008-5077`

Medium (CVSS: 5.8)
NVT: Slackware Advisory SSA:2009-014-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2009-014-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-014-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue when connecting to an SSL/TLS server that uses a certificate containing a DSA or ECDSA key.
More details about this issue may be found here: http://www.openssl.org/news/secadv_20090107.txt
http://www.ocert.org/advisories/ocert-2008-016.html

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-014-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.63232

... continues on next page ...

... continued from previous page ...

Version used: `$Revision: 5999 $`

References
`CVE: CVE-2008-5077`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2009-014-02 bind

Summary
The remote host is missing an update as announced via advisory SSA:2009-014-02.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-014-02

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.
More details about this issue may be found here: https://www.isc.org/node/373 http://www.ocert.org/advisories/ocert-2008-016.html

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-014-02 bind`
OID:1.3.6.1.4.1.25623.1.0.63231
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2008-5077, CVE-2009-0025`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2009-014-02 bind

Summary
The remote host is missing an update as announced via advisory SSA:2009-014-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-014-02

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.
More details about this issue may be found here: https://www.isc.org/node/373 http://www.ocert.org/advisories/ocert-2008-016.html

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-014-02 bind`
OID:1.3.6.1.4.1.25623.1.0.63231
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2008-5077, CVE-2009-0025`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2009-015-01 bind 10.2/11.0 recompile

Summary
The remote host is missing an update as announced via advisory SSA:2009-015-01.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-015-01

Vulnerability Insight
Updated bind packages are available for Slackware 10.2 and 11.0 to address a load problem. It was reported that the initial build of these updates complained that the Linux capability module was not present and would refuse to load. It was determined that the packages which were compiled on 10.2 and 11.0 systems running 2.6 kernels, and although the installed kernel headers are from 2.4.x, it picked up on this resulting in packages that would only run under 2.4 kernels. These new packages address the issue.
As always, any problems noted with update patches should be reported to security@slackware.com, and we will do our best to address them as quickly as possible.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-015-01 bind 10.2/11.0 recompile`
OID:1.3.6.1.4.1.25623.1.0.63229
Version used: `$Revision: 5888 $`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2009-015-01 bind 10.2/11.0 recompile

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update as announced via advisory SSA:2009-015-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-015-01

Vulnerability Insight
Updated bind packages are available for Slackware 10.2 and 11.0 to address a load problem. It was reported that the initial build of these updates complained that the Linux capability module was not present and would refuse to load. It was determined that the packages which were compiled on 10.2 and 11.0 systems running 2.6 kernels, and although the installed kernel headers are from 2.4.x, it picked up on this resulting in packages that would only run under 2.4 kernels. These new packages address the issue.
As always, any problems noted with update patches should be reported to security@slackware.com, and we will do our best to address them as quickly as possible.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-015-01 bind 10.2/11.0 recompile`
OID:1.3.6.1.4.1.25623.1.0.63229
Version used: `$Revision: 5888 $`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2009-051-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2009-051-01.

Vulnerability Detection Result
`Package libpng-1.2.12-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-051-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-051-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.63429
Version used: `$Revision: 5977 $`

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2009-0040

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2009-051-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2009-051-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-051-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2009-051-01 libpng
OID:1.3.6.1.4.1.25623.1.0.63429
Version used: $Revision: 5977 $

References
CVE: CVE-2009-0040

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2009-069-01 curl

Summary
The remote host is missing an update as announced via advisory SSA:2009-069-01.

Vulnerability Detection Result
Package curl-7.15.5-i386-1 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-069-01

Vulnerability Insight
New curl packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-069-01 curl`
OID:1.3.6.1.4.1.25623.1.0.63561
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2009-0037`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2009-069-01 curl

Summary
The remote host is missing an update as announced via advisory SSA:2009-069-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-069-01

Vulnerability Insight
New curl packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-069-01 curl`
OID:1.3.6.1.4.1.25623.1.0.63561
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2009-0037`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2009-120-01 ruby

Summary
The remote host is missing an update as announced via advisory SSA:2009-120-01.

Vulnerability Detection Result
`Package ruby-1.8.4-i686-1kjz is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-120-01

Vulnerability Insight
New ruby packages are available for Slackware 11.0, 12.0, 12.1, 12.2, and -current to fix a problem with REXML and other security issues.
For details about the REXML issue, see:
http://www.ruby-lang.org/en/news/2008/08/23/dos-vulnerability-in-rexml/
A full list may be found in the ChangeLog file included with the source code.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-120-01 ruby`
OID:1.3.6.1.4.1.25623.1.0.63941
Version used: `$Revision: 5912 $`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2009-120-01 ruby

Summary
The remote host is missing an update as announced via advisory SSA:2009-120-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-120-01

Vulnerability Insight
New ruby packages are available for Slackware 11.0, 12.0, 12.1, 12.2, and -current to fix a problem with REXML and other security issues.
For details about the REXML issue, see:
http://www.ruby-lang.org/en/news/2008/08/23/dos-vulnerability-in-rexml/
A full list may be found in the ChangeLog file included with the source code.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-120-01 ruby`
OID:1.3.6.1.4.1.25623.1.0.63941
Version used: `$Revision: 5912 $`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2009-170-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2009-170-01.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`Package libpng-1.2.12-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-170-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.
Jeff Phillips discovered an uninitialized-memory-read bug affecting interlaced images that may have security implications.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-170-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.64258
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2009-2042`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2009-170-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2009-170-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-170-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.
Jeff Phillips discovered an uninitialized-memory-read bug affecting interlaced images that may have security implications.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-170-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.64258
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2009-2042`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2009-170-02 ruby

Summary
The remote host is missing an update as announced via advisory SSA:2009-170-02.

Vulnerability Detection Result
`Package ruby-1.8.4-i686-1kjz is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-170-02

Vulnerability Insight
New ruby packages are available for Slackware 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-170-02 ruby`
OID:1.3.6.1.4.1.25623.1.0.64257
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2009-1904`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2009-170-02 ruby

Summary
The remote host is missing an update as announced via advisory SSA:2009-170-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-170-02

Vulnerability Insight
New ruby packages are available for Slackware 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-170-02 ruby`
OID:1.3.6.1.4.1.25623.1.0.64257
Version used: `$Revision: 5912 $`

. . . continues on next page . . .

... continued from previous page ...

References
CVE: CVE-2009-1904

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2009-210-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2009-210-01.

Vulnerability Detection Result
Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-210-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.
ISC has published an announcement here:
https://www.isc.org/node/479
And CERT has published an advisory here:
http://www.kb.cert.org/vuls/id/725188

Vulnerability Detection Method
Details:Slackware Advisory SSA:2009-210-01 bind
OID:1.3.6.1.4.1.25623.1.0.64569
Version used: $Revision: 5958 $

References
CVE: CVE-2009-0696

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2009-210-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2009-210-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-210-01

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, and -current to fix a security issue.
ISC has published an announcement here:
https://www.isc.org/node/479
And CERT has published an advisory here:
http://www.kb.cert.org/vuls/id/725188

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-210-01 bind`
OID:1.3.6.1.4.1.25623.1.0.64569
Version used: `$Revision: 5958 $`

References
`CVE: CVE-2009-0696`

Medium (CVSS: 6.0)
NVT: Slackware Advisory SSA:2009-276-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2009-276-01.

Vulnerability Detection Result
`Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-276-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-276-01 samba`
OID:1.3.6.1.4.1.25623.1.0.65009
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2009-2813, CVE-2009-2948, CVE-2009-2906`

Medium (CVSS: 6.0)
NVT: Slackware Advisory SSA:2009-276-01 samba

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update as announced via advisory SSA:2009-276-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-276-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-276-01 samba`
OID:1.3.6.1.4.1.25623.1.0.65009
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2009-2813, CVE-2009-2948, CVE-2009-2906`

Medium (CVSS: 5.8)
NVT: Slackware Advisory SSA:2009-320-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2009-320-01.

Vulnerability Detection Result
`Package openssl-0.9.8d-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-320-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-320-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.66270
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2009-3555`

Medium (CVSS: 5.8)
NVT: Slackware Advisory SSA:2009-320-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2009-320-01.

Vulnerability Detection Result
`Package openssl-solibs-0.9.8d-i486-1 is installed which is known to be vulnerabl`
`↪e.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-320-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-320-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.66270
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2009-3555`

Medium (CVSS: 5.8)
NVT: Slackware Advisory SSA:2009-320-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2009-320-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-320-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-320-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.66270
Version used: `$Revision: 5940 $`

. . . continues on next page . . .

... continued from previous page ...

References
CVE: CVE-2009-3555

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2010-090-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-090-01.

Vulnerability Detection Result
Package openssl-0.9.8d-i486-1 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-090-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.
A recompiled proftpd package is required if you run ProFTPD.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2010-090-01 openssl
OID:1.3.6.1.4.1.25623.1.0.67216
Version used: $Revision: 5988 $

References
CVE: CVE-2010-0433, CVE-2010-0740

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2010-090-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-090-01.

Vulnerability Detection Result
Package openssl-solibs-0.9.8d-i486-1 is installed which is known to be vulnerabl
↪e.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-090-01

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.
A recompiled proftpd package is required if you run ProFTPD.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-090-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.67216
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2010-0433, CVE-2010-0740`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2010-090-01 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2010-090-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-090-01

Vulnerability Insight
New openssl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.
A recompiled proftpd package is required if you run ProFTPD.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-090-01 openssl`
OID:1.3.6.1.4.1.25623.1.0.67216
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2010-0433, CVE-2010-0740`

Medium (CVSS: 6.9)
NVT: Slackware Advisory SSA:2010-110-01 sudo

Summary
The remote host is missing an update as announced via advisory SSA:2010-110-01.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Package sudo-1.6.8-i386-1 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-110-01

Vulnerability Insight
New sudo packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2010-110-01 sudo
OID:1.3.6.1.4.1.25623.1.0.67346
Version used: $Revision: 5931 $

References
CVE: CVE-2010-0426, CVE-2010-1163

Medium (CVSS: 6.9)
NVT: Slackware Advisory SSA:2010-110-01 sudo

Summary
The remote host is missing an update as announced via advisory SSA:2010-110-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-110-01

Vulnerability Insight
New sudo packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2010-110-01 sudo
OID:1.3.6.1.4.1.25623.1.0.67346
Version used: $Revision: 5931 $

References
CVE: CVE-2010-0426, CVE-2010-1163

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2010-176-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2010-176-01.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-176-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues when DNSSEC is enabled (which is not the default setting).

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-176-01 bind`
OID:1.3.6.1.4.1.25623.1.0.68170
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2009-4022, CVE-2010-0097`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2010-176-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2010-176-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-176-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues when DNSSEC is enabled (which is not the default setting).

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details:Slackware Advisory SSA:2010-176-01 bind
OID:1.3.6.1.4.1.25623.1.0.68170
Version used: $Revision: 5940 $

References
CVE: CVE-2009-4022, CVE-2010-0097

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2010-180-02 libtiff

Summary
The remote host is missing an update as announced via advisory SSA:2010-180-02.

Vulnerability Detection Result
Package libtiff-3.8.2-i486-2 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-180-02

Vulnerability Insight
New libtiff packages are available for Slackware 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2010-180-02 libtiff
OID:1.3.6.1.4.1.25623.1.0.68164
Version used: $Revision: 5958 $

References
CVE: CVE-2010-1411, CVE-2010-2065, CVE-2010-2067

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2010-180-02 libtiff

Summary
The remote host is missing an update as announced via advisory SSA:2010-180-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-180-02

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
New libtiff packages are available for Slackware 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-180-02 libtiff`
OID:1.3.6.1.4.1.25623.1.0.68164
Version used: `$Revision: 5958 $`

References
`CVE: CVE-2010-1411, CVE-2010-2065, CVE-2010-2067`

Medium (CVSS: 6.2)
NVT: Slackware Advisory SSA:2010-257-02 sudo

Summary
The remote host is missing an update as announced via advisory SSA:2010-257-02.

Vulnerability Detection Result
`Package sudo-1.6.8-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-257-02

Vulnerability Insight
New sudo packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-257-02 sudo`
OID:1.3.6.1.4.1.25623.1.0.68179
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2010-2956`

Medium (CVSS: 6.2)
NVT: Slackware Advisory SSA:2010-257-02 sudo

Summary
The remote host is missing an update as announced via advisory SSA:2010-257-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-257-02

Vulnerability Insight
New sudo packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-257-02 sudo`
OID:1.3.6.1.4.1.25623.1.0.68179
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2010-2956`

Medium (CVSS: 5.1)
NVT: Slackware Advisory SSA:2010-263-01 bzip2

Summary
The remote host is missing an update as announced via advisory SSA:2010-263-01.

Vulnerability Detection Result
`Package bzip2-1.0.3-i486-3 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-263-01

Vulnerability Insight
New bzip2 packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-263-01 bzip2`
OID:1.3.6.1.4.1.25623.1.0.68177
Version used: `$Revision: 5950 $`

References
`CVE: CVE-2010-0405`

Medium (CVSS: 5.1)
NVT: Slackware Advisory SSA:2010-263-01 bzip2

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update as announced via advisory SSA:2010-263-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-263-01

Vulnerability Insight
New bzip2 packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-263-01 bzip2`
OID:1.3.6.1.4.1.25623.1.0.68177
Version used: `$Revision: 5950 $`

References
`CVE: CVE-2010-0405`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2010-324-01 xpdf

Summary
The remote host is missing an update as announced via advisory SSA:2010-324-01.

Vulnerability Detection Result
`Package xpdf-3.01-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-324-01

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-324-01 xpdf`
OID:1.3.6.1.4.1.25623.1.0.68675
Version used: `$Revision: 5977 $`

References
`CVE: CVE-2010-3702, CVE-2010-3703, CVE-2010-3704`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2010-324-01 xpdf

Summary
The remote host is missing an update as announced via advisory SSA:2010-324-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-324-01

Vulnerability Insight
New xpdf packages are available for Slackware 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-324-01 xpdf`
OID:1.3.6.1.4.1.25623.1.0.68675
Version used: `$Revision: 5977 $`

References
`CVE: CVE-2010-3702, CVE-2010-3703, CVE-2010-3704`

Medium (CVSS: 6.4)
NVT: Slackware Advisory SSA:2010-350-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2010-350-01.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-350-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues that could allow attackers to successfully query private DNS records, or cause a denial of service.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-350-01 bind`
OID:1.3.6.1.4.1.25623.1.0.68667
Version used: `$Revision: 5988 $`

. . . continues on next page . . .

... continued from previous page ...

References
CVE: CVE-2010-3613, CVE-2010-3614, CVE-2010-3615

Medium (CVSS: 6.4)
NVT: Slackware Advisory SSA:2010-350-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2010-350-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-350-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues that could allow attackers to successfully query private DNS records, or cause a denial of service.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2010-350-01 bind
OID:1.3.6.1.4.1.25623.1.0.68667
Version used: $Revision: 5988 $

References
CVE: CVE-2010-3613, CVE-2010-3614, CVE-2010-3615

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2010-357-02 proftpd

Summary
The remote host is missing an update as announced via advisory SSA:2010-357-02.

Vulnerability Detection Result
Package proftpd-1.3.0a-i386-1 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-357-02

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

New proftpd packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-357-02 proftpd`
OID:1.3.6.1.4.1.25623.1.0.68801
Version used: `$Revision: 5977 $`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2010-357-02 proftpd

Summary
The remote host is missing an update as announced via advisory SSA:2010-357-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2010-357-02

Vulnerability Insight
New proftpd packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2010-357-02 proftpd`
OID:1.3.6.1.4.1.25623.1.0.68801
Version used: `$Revision: 5977 $`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-041-04 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2011-041-04.

Vulnerability Detection Result
`Package openssl-0.9.8d-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-041-04

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

New openssl packages are available for 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-041-04 openssl`
OID:1.3.6.1.4.1.25623.1.0.68921
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2011-0014`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-041-04 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2011-041-04.

Vulnerability Detection Result
`Package openssl-solibs-0.9.8d-i486-1 is installed which is known to be vulnerabl`
`↪e.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-041-04

Vulnerability Insight
New openssl packages are available for 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-041-04 openssl`
OID:1.3.6.1.4.1.25623.1.0.68921
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2011-0014`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-041-04 openssl

Summary
The remote host is missing an update as announced via advisory SSA:2011-041-04.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-041-04

Vulnerability Insight
New openssl packages are available for 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-041-04 openssl`
OID:1.3.6.1.4.1.25623.1.0.68921
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2011-0014`

Medium (CVSS: 4.4)
NVT: Slackware Advisory SSA:2011-041-05 sudo

Summary
The remote host is missing an update as announced via advisory SSA:2011-041-05.

Vulnerability Detection Result
`Package sudo-1.6.8-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-041-05

Vulnerability Insight
New sudo packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-041-05 sudo`
OID:1.3.6.1.4.1.25623.1.0.68920
Version used: `$Revision: 5958 $`

References
`CVE: CVE-2011-0010`

Medium (CVSS: 4.4)
NVT: Slackware Advisory SSA:2011-041-05 sudo

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update as announced via advisory SSA:2011-041-05.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-041-05

Vulnerability Insight
New sudo packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-041-05 sudo`
OID:1.3.6.1.4.1.25623.1.0.68920
Version used: `$Revision: 5958 $`

References
`CVE: CVE-2011-0010`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-059-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2011-059-01.

Vulnerability Detection Result
`Package samba-3.0.14a-i486-1ron is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-059-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a denial of service security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-059-01 samba`
OID:1.3.6.1.4.1.25623.1.0.69122
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2011-0719`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-059-01 samba

Summary
The remote host is missing an update as announced via advisory SSA:2011-059-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-059-01

Vulnerability Insight
New samba packages are available for Slackware 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a denial of service security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-059-01 samba`
OID:1.3.6.1.4.1.25623.1.0.69122
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2011-0719`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-095-01 proftpd

Summary
The remote host is missing an update as announced via advisory SSA:2011-095-01.

Vulnerability Detection Result
`Package proftpd-1.3.0a-i386-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-095-01

Vulnerability Insight
New proftpd packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-095-01 proftpd`
OID:1.3.6.1.4.1.25623.1.0.69584
Version used: `$Revision: 5977 $`

. . . continues on next page . . .

... continued from previous page ...

References
CVE: CVE-2011-1137

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-095-01 proftpd

Summary
The remote host is missing an update as announced via advisory SSA:2011-095-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-095-01

Vulnerability Insight
New proftpd packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2011-095-01 proftpd
OID:1.3.6.1.4.1.25623.1.0.69584
Version used: $Revision: 5977 $

References
CVE: CVE-2011-1137

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2011-110-01 rdesktop

Summary
The remote host is missing an update as announced via advisory SSA:2011-110-01.

Vulnerability Detection Result
Package rdesktop-1.5.0-i486-1 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-110-01

Vulnerability Insight
New rdesktop packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-110-01 rdesktop`
OID:1.3.6.1.4.1.25623.1.0.69576
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2011-1595`

Medium (CVSS: 4.3)
NVT: Slackware Advisory SSA:2011-110-01 rdesktop

Summary
The remote host is missing an update as announced via advisory SSA:2011-110-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-110-01

Vulnerability Insight
New rdesktop packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-110-01 rdesktop`
OID:1.3.6.1.4.1.25623.1.0.69576
Version used: `$Revision: 5931 $`

References
`CVE: CVE-2011-1595`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-147-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2011-147-01.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-147-01

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-147-01 bind`
OID:1.3.6.1.4.1.25623.1.0.71944
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2011-1910`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-147-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2011-147-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-147-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-147-01 bind`
OID:1.3.6.1.4.1.25623.1.0.71944
Version used: `$Revision: 5956 $`

References
`CVE: CVE-2011-1910`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-210-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2011-210-01.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Package libpng-1.2.12-i486-2 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-210-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2011-210-01 libpng
OID:1.3.6.1.4.1.25623.1.0.71955
Version used: $Revision: 5931 $

References
CVE: CVE-2004-0421, CVE-2011-0421

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-210-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2011-210-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-210-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2011-210-01 libpng
OID:1.3.6.1.4.1.25623.1.0.71955
Version used: $Revision: 5931 $

References
CVE: CVE-2004-0421, CVE-2011-0421

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-224-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2011-224-01.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-224-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-224-01 bind`
OID:1.3.6.1.4.1.25623.1.0.71963
Version used: `$Revision: 5912 $`

References
`CVE: CVE-2011-1910, CVE-2011-2464`

Medium (CVSS: 5.0)
NVT: Slackware Advisory SSA:2011-224-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2011-224-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-224-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-224-01 bind`
OID:1.3.6.1.4.1.25623.1.0.71963

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 5912 $

References
CVE: CVE-2011-1910, CVE-2011-2464

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2012-098-01 libtiff

Summary
The remote host is missing an update as announced via advisory SSA:2012-098-01.

Vulnerability Detection Result
Package libtiff-3.8.2-i486-2 is installed which is known to be vulnerable.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-098-01

Vulnerability Insight
New libtiff packages are available for Slackware 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:Slackware Advisory SSA:2012-098-01 libtiff
OID:1.3.6.1.4.1.25623.1.0.71988
Version used: $Revision: 5963 $

References
CVE: CVE-2012-1173

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2012-098-01 libtiff

Summary
The remote host is missing an update as announced via advisory SSA:2012-098-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-098-01

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

New libtiff packages are available for Slackware 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2012-098-01 libtiff`
OID:1.3.6.1.4.1.25623.1.0.71988
Version used: `$Revision: 5963 $`

References
`CVE: CVE-2012-1173`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2012-206-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2012-206-01.

Vulnerability Detection Result
`Package libpng-1.2.12-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-206-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2012-206-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.71970
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2011-3045, CVE-2011-3048, CVE-2012-3386`

Medium (CVSS: 6.8)
NVT: Slackware Advisory SSA:2012-206-01 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2012-206-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2012-206-01

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, 13.37, and -current to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2012-206-01 libpng`
OID:1.3.6.1.4.1.25623.1.0.71970
Version used: `$Revision: 6022 $`

References
`CVE: CVE-2011-3045, CVE-2011-3048, CVE-2012-3386`

Medium (CVSS: 4.3)
NVT: Snort 'IPv6' Packet Denial Of Service Vulnerability (Linux)

Summary
This host has Snort installed and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attacker to crash an affected application, creating a denial of service condition. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Snort version 2.8.5.1 or later For updates, Refer http://www.snort.org/downloads

Affected Software/OS
Snort version prior to 2.8.5.1 on Linux.

Vulnerability Insight
This flaw is caused by an error when processing malformed IPv6 packets when the application is compiled with the '–enable-ipv6' option and is running in verbose mode (-v).

Vulnerability Detection Method
Details:`Snort 'IPv6' Packet Denial Of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.801139
Version used: `$Revision: 4869 $`

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2009-3641
BID:36795
Other:
URL:http://secunia.com/advisories/37135
URL:http://xforce.iss.net/xforce/xfdb/53912
URL:http://www.vupen.com/english/advisories/2009/3014
URL:https://bugzilla.redhat.com/show_bug.cgi?id=530863

Medium (CVSS: 6.8)
NVT: Sun Java SE Unspecified Vulnerability In JDK/JRE/SDK - Aug09

Summary
This host is installed with Sun Java JDK/JRE/SDK and is prone to unspecified vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker may leverage this issue by modifying or creating of files on the affected application.
Impact Level: System/Application

Solution
Upgrade to JDK/JRE version 6 Update 15 or 5 Update 20 http://java.sun.com/javase/downloads/index.jsp http://java.sun.com/javase/downloads/index_jdk5.jsp or Upgrade to SDK/JRE version 1.4.2_22 http://java.sun.com/j2se/1.4.2/download.html or Apply the patch from below link, http://sunsolve.sun.com/search/document.do?assetkey=1-21-125136-16-1
*** NOTE: Ignore this warning if above mentioned patch is already applied. *****

Affected Software/OS
Sun Java JDK/JRE version 6 before Update 15 or 5.0 before Update 20 Sun Java SDK/JRE version prior to 1.4.2_22

Vulnerability Insight
Unspecified vulnerability exists in 'JNLPAppletlauncher' class, which can be exploited via vectors involving an untrusted Java applet.

Vulnerability Detection Method
Details:Sun Java SE Unspecified Vulnerability In JDK/JRE/SDK - Aug09
OID:1.3.6.1.4.1.25623.1.0.800869
Version used: $Revision: 4869 $

References
CVE: CVE-2009-2676
BID:35946
Other:

... continues on next page ...

... continued from previous page ...

URL:http://secunia.com/advisories/36159
URL:http://sunsolve.sun.com/search/document.do?assetkey=1-66-263490-1

Medium (CVSS: 5.0)
NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability

Summary
The host is running TCP services and is prone to denial of service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

Solution
Please see the referenced advisories for more information on obtaining and applying fixes.

Affected Software/OS
TCP/IP v4

Vulnerability Insight
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

Vulnerability Detection Method
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not.
Details:TCP Sequence Number Approximation Reset Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902815
Version used: $Revision: 5912 $

References
CVE: CVE-2004-0230
BID:10183
Other:
URL:http://xforce.iss.net/xforce/xfdb/15886
URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006
URL:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx
URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx
URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html

Medium (CVSS: 5.8)
NVT: Tor 'Relay Early' Traffic Confirmation Attack Vunerability oct14 (Linux)

Product detection result
cpe:/a:tor:tor:0.1.1.26.
Detected by Tor Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.900418)

Summary
This host is installed with Tor browser and is prone to information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to manipulate protocol headers and perform traffic confirmation attack.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 0.2.4.23 or 0.2.5.6-alpha or later, For updates refer to https://www.torproject.org

Affected Software/OS
Tor browser before 0.2.4.23 and 0.2.5 before 0.2.5.6-alpha on Linux

Vulnerability Insight
Flaw exists due to an error in the handling of sequences of Relay and Relay Early commands.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:Tor 'Relay Early' Traffic Confirmation Attack Vunerability oct14 (Linux)
OID:1.3.6.1.4.1.25623.1.0.804934
Version used: $Revision: 3555 $

Product Detection Result
Product: cpe:/a:tor:tor:0.1.1.26.
Method: Tor Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.900418)

References
CVE: CVE-2014-5117
BID:68968
Other:
URL:http://xforce.iss.net/xforce/xfdb/95053
URL:https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffi

... continues on next page ...

... continued from previous page ...

↪c-confirmation-attack

Medium (CVSS: 6.8)
NVT: VLC Media Player '.AVI' File BOF Vulnerability (Linux)

Summary
The host is installed with VLC Media Player and is prone to buffer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attackers to execute arbitrary code in the context of the application. Failed attacks will cause denial-of-service conditions. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to the VLC media player version 1.1.11 or later, For updates refer to http://www.videolan.org/

Affected Software/OS
VLC media player version prior to 1.1.11 on Linux.

Vulnerability Insight
The flaw is due to an integer underflow error when parsing the 'strf' chunk within AVI files can be exploited to cause a heap-based buffer overflow.

Vulnerability Detection Method
Details:VLC Media Player '.AVI' File BOF Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.902707
Version used: $Revision: 5351 $

References
CVE: CVE-2011-2588
BID:48664
Other:
URL:http://secunia.com/advisories/45066
URL:http://xforce.iss.net/xforce/xfdb/68532
URL:http://www.videolan.org/security/sa1106.html

Medium (CVSS: 6.8)
NVT: VLC Media Player 'AMV' Denial of Service Vulnerability (Linux)

Summary
The host is installed with VLC Media Player and is prone to denial of service vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attackers to cause a denial of service or possibly execute arbitrary code via a malformed AMV file.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to VLC media player version 1.1.10 or later, For updates refer to http://www.videolan.org/vlc/

Affected Software/OS
VLC media player version 1.1.9 and prior on Linux.

Vulnerability Insight
The flaw is due to error while handling 'sp5xdec.c' in the Sunplus SP5X JPEG decoder in libavcodec, performs a write operation outside the bounds of an unspecified array.

Vulnerability Detection Method
Details:`VLC Media Player 'AMV' Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.802118
Version used: `$Revision: 3117 $`

References
`CVE: CVE-2011-1931`
`BID:47602`
`Other:`
`URL:http://www.securityfocus.com/archive/1/517706`
`URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=624339`

Medium (CVSS: 6.8)
NVT: VLC Media Player 'MP4_ReadBox_skcr()' Buffer Overflow Vulnerability (Linux)

Summary
The host is installed with VLC Media Player and is prone buffer overflow vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow attackers to execute arbitrary code by tricking a user into opening a malicious file or visiting a specially crafted web page. Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to the VLC media player version 1.1.9 or later, For updates refer to http://download.videolan.org/pub/videolan/vlc/

Affected Software/OS
VLC media player version prior to 1.1.9 on Linux

Vulnerability Insight
The flaw is caused by a heap corruption error in the 'MP4_ReadBox_skcr()' [modules/demux/mp4/libmp4.c] function when processing malformed MP4 (MPEG-4 Part 14) data.

Vulnerability Detection Method
Details:VLC Media Player 'MP4_ReadBox_skcr()' Buffer Overflow Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.801783
Version used: $Revision: 5351 $

References
CVE: CVE-2011-1684
BID:47293
Other:
URL:http://secunia.com/advisories/44022
URL:http://xforce.iss.net/xforce/xfdb/66664
URL:http://www.vupen.com/english/advisories/2011/0916

Medium (CVSS: 6.8)
NVT: VLC Media Player 3GP File Denial of Service Vulnerability Oct15 (Linux)

Product detection result
cpe:/a:videolan:vlc_media_player:0.8.4a:a
Detected by VLC Media Player Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1
↪.0.900529)

Summary
The host is installed with VLC media player and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 0.8.4aa
Fixed version: NoneAvailable

Impact
Successful exploitation will allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted 3GP file.
Impact Level: System/Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: NoneAvailable
No updates are available at the moment, For updates refer to http://www.videolan.org

Affected Software/OS
VideoLAN VLC media player 2.2.1 and earlier on Linux.

Vulnerability Insight
The flaw is due to insufficient restrictions on a writable buffer which affects the 3GP file format parser.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`VLC Media Player 3GP File Denial of Service Vulnerability Oct15 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.806087
Version used: `$Revision: 2513 $`

Product Detection Result
Product: `cpe:/a:videolan:vlc_media_player:0.8.4a:a`
Method: `VLC Media Player Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900529)

References
`CVE: CVE-2015-5949`
`BID:76448`
`Other:`
`URL:https://packetstormsecurity.com/files/133266`
`URL:http://www.securityfocus.com/archive/1/archive/1/536287/100/0/threaded`

Medium (CVSS: 4.3)
NVT: VLC Media Player ASF Demuxer Denial of Service Vulnerability (Linux)

Product detection result
`cpe:/a:videolan:vlc_media_player:0.8.4a:a`
`Detected by VLC Media Player Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1`
`↪.0.900529)`

Summary
This host is installed with VLC Media Player and is prone to denial of service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow attackers to cause a denial of service condition.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to VLC media player version 2.1.3 or later, For updates refer to http://www.videolan.org/vlc

Affected Software/OS
VLC media player version 2.1.2 and prior on Linux.

Vulnerability Insight
The flaw exist due to a divide-by-zero error when processing malicious '.asf' files.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`VLC Media Player ASF Demuxer Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804325
Version used: `$Revision: 3555 $`

Product Detection Result
Product: `cpe:/a:videolan:vlc_media_player:0.8.4a:a`
Method: `VLC Media Player Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900529)

References
`CVE: CVE-2014-1684`
`BID:65399`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/90955`
`URL:http://www.exploit-db.com/exploits/31429`
`URL:http://www.videolan.org/developers/vlc-branch/NEWS`
`URL:http://packetstormsecurity.com/files/125080/VLC-Media-Player-2.1.2-Denial-Of-Service.html`

Medium (CVSS: 4.3)
NVT: VLC Media Player Denial of Service Vulnerability Mar14 (Linux)

Product detection result
`cpe:/a:videolan:vlc_media_player:0.8.4a:a`
`Detected by VLC Media Player Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.900529)`

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with VLC Media Player and is prone to denial of service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to cause a denial of service conditions.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to VLC media player version 2.0.7 or later, For updates refer to http://www.videolan.org/vlc

Affected Software/OS
VLC media player version 2.0.6 and prior on Linux.

Vulnerability Insight
The flaw exist due to some unspecified error.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`VLC Media Player Denial of Service Vulnerability Mar14 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.804348
Version used: `$Revision: 3555 $`

Product Detection Result
Product: `cpe:/a:videolan:vlc_media_player:0.8.4a:a`
Method: `VLC Media Player Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.900529)

References
`CVE: CVE-2013-7340`
`Other:`
`URL:http://www.videolan.org/developers/vlc-branch/NEWS`

Medium (CVSS: 5.0)
NVT: VLC Media Player Meta-Information Denial of Service Vulnerability (Linux)

Summary
The host is installed with VLC Media Player and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation could allow attackers to crash the affected application, denying service to legitimate users. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to the VLC media player version 1.1.3 or later, For updates refer to http://www.videolan.org/vlc/

Affected Software/OS
VLC media player version prior to 1.1.3 on Linux.

Vulnerability Insight
The flaw is due to an input validation error when trying to extract meta-informations about input media through 'ID3v2' tags.

Vulnerability Detection Method
Details:`VLC Media Player Meta-Information Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.801430
Version used: `$Revision: 5388 $`

References
`CVE: CVE-2010-2937`
`BID:42386`
`Other:`
`URL:http://seclists.org/oss-sec/`
`URL:http://www.videolan.org/security/sa1004.html`
`URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=592669`

Medium (CVSS: 5.0)
NVT: VLC Media Player Stack Overflow Vulnerability (Lin-Mar09)

Summary
This host is installed with VLC Media Player and is prone to Stack Overflow Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows the attacker to execute arbitrary codes with escalated privileges and cause overflow in stack. Impact Level: Application

Solution
Upgrade to VLC media player version 1.0 or later, For updates refer to http://www.videolan.org/vlc

... continues on next page ...

... continued from previous page ...

Affected Software/OS
VLC media player 0.9.8a and prior on Linux.

Vulnerability Insight
This flaw is due to improper boundary checking in status.xml in the web interface by an overly long request.

Vulnerability Detection Method
Details:`VLC Media Player Stack Overflow Vulnerability (Lin-Mar09)`
OID:1.3.6.1.4.1.25623.1.0.900531
Version used: `$Revision: 5148 $`

References
`CVE: CVE-2009-1045`
`BID:34126`
`Other:`
`URL:http://www.milw0rm.com/exploits/8213`
`URL:http://xforce.iss.net/xforce/xfdb/49249`
`URL:http://bugs.gentoo.org/show_bug.cgi?id=262708`
`URL:http://www.openwall.com/lists/oss-security/2009/03/17/4`

Medium (CVSS: 6.8)
NVT: VLC Media Player XSPF Playlist Memory Corruption Vulnerability (Linux)

Summary
This host is installed with VLC Media Player and is prone to Memory Corruption Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows attackers to execute arbitrary code by tricking a user into opening a specially crafted XSPF file or even can crash an affected application. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Version 0.9.3 or later, http://www.videolan.org/vlc/

Affected Software/OS
VLC media player 0.9.2 and prior Linux.

Vulnerability Insight
The flaw exists due to VLC (xspf.c) library does not properly perform bounds checking on an identifier tag from an XSPF file before using it to index an array on the heap.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details:VLC Media Player XSPF Playlist Memory Corruption Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.800113
Version used: $Revision: 5158 $

References
CVE: CVE-2008-4558
BID:31758
Other:
URL:http://secunia.com/advisories/32267/
URL:http://www.frsirt.com/english/advisories/2008/2826/products
URL:http://www.coresecurity.com/content/vlc-xspf-memory-corruption

Medium (CVSS: 5.0)
NVT: Wireshark Multiple Vulnerabilities - July08 (Linux)

Summary
The host is running Wireshark/Ethereal, which is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could result in application crash, disclose of system memory, and an incomplete syslog encapsulated packets. Impact Level : SYSTEM

Solution
Upgrade to wireshark to 1.0.1 or later. http://www.wireshark.org/download.html

Affected Software/OS
Wireshark versions prior to 1.0.1 on Linux (All).
Quick Fix : Disable the following dissectors, GSM SMS, PANA, KISMET, RTMPT, and RMI

Vulnerability Insight
The flaws exists due to errors in GSM SMS dissector, PANA and KISMET dissectors, RTMPT dissector, RMI dissector, and in syslog dissector.

Vulnerability Detection Method
Details:Wireshark Multiple Vulnerabilities - July08 (Linux)
OID:1.3.6.1.4.1.25623.1.0.900011
Version used: $Revision: 4557 $

References
CVE: CVE-2008-1561, CVE-2008-1562, CVE-2008-1563
BID:28485

[return to 192.168.27.45]

2.1.5 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH Denial of Service Vulnerability

Summary
OpenSSH is prone to a remote denial-of-service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Exploiting this issue allows remote attackers to trigger denial-of- service conditions.

Solution
Updates are available.

Affected Software/OS
OpenSSH 6.1 and prior

Vulnerability Insight
The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

Vulnerability Detection Method
Compare the version retrieved from the banner with the affected range.
Details:`OpenSSH Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103939
Version used: `$Revision: 4336 $`

References
`CVE: CVE-2010-5107`
`BID:58162`
`Other:`
`URL:http://www.securityfocus.com/bid/58162`
`URL:http://www.openssh.com`

Medium (CVSS: 5.8)
NVT: OpenSSH 'child_set_env()' Function Security Bypass Vulnerability

Summary
OpenSSH is prone to a security-bypass vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

Impact
The security bypass allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.

Solution
Updates are available.

Affected Software/OS
Versions prior to OpenSSH 6.6 are vulnerable.

Vulnerability Insight
sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config.

Vulnerability Detection Method
Check the version.
Details:`OpenSSH 'child_set_env()' Function Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105003
Version used: `$Revision: 4336 $`

References
```
CVE: CVE-2014-2532
BID:66355
Other:
  URL:http://www.securityfocus.com/bid/66355
   URL:http://www.openssh.com
```

Medium (CVSS: 5.5)
NVT: OpenSSH <= 7.2p1 - Xauth Injection

Product detection result
```
cpe:/a:openbsd:openssh:4.4
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
```

Summary
openssh xauth command injection may lead to forced-command and /bin/false bypass

Vulnerability Detection Result
```
Installed version: 4.4
Fixed version:     7.2p2
```

Impact
By injecting xauth commands one gains limited* read/write arbitrary files, information leakage or xauth-connect capabilities.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.2p2 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions before 7.2p2

Vulnerability Insight
An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie. The newline acts as a command separator to the xauth binary. This attack requires the server to have 'X11Forwarding yes' enabled. Disabling it, mitigates this vector.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH <= 7.2p1 - Xauth Injection`
OID:1.3.6.1.4.1.25623.1.0.105581
Version used: `$Revision: 5745 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.4`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2016-3115`
`Other:`
`URL:http://www.openssh.com/txt/release-7.2p2`

Medium (CVSS: 5.8)
NVT: OpenSSH Certificate Validation Security Bypass Vulnerability

Summary
OpenSSH is prone to a security-bypass vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Attackers can exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks.

Solution
Updates are available.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSH 6.6 and prior are vulnerable.

Vulnerability Insight
The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.

Vulnerability Detection Method
Check the version
Details:`OpenSSH Certificate Validation Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105004
Version used: `$Revision: 4336 $`

References
`CVE: CVE-2014-2653`
`BID:66459`
`Other:`
`URL:http://www.securityfocus.com/bid/66459`
`URL:http://www.openssh.com`

Medium (CVSS: 5.0)
NVT: OpenSSH Denial of Service Vulnerability - Jan16

Product detection result
`cpe:/a:openbsd:openssh:4.4`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 4.4`
`Fixed version: 7.1p2`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read and application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.1p2 or later. For updates refer to http://www.openssh.com

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSH versions before 7.1p2

Vulnerability Insight
The flaw exists due to an error in 'ssh_packet_read_poll2' function within 'packet.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH Denial of Service Vulnerability - Jan16`
OID:1.3.6.1.4.1.25623.1.0.806671
Version used: `$Revision: 5650 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.4`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2016-1907`
`Other:`
`URL:http://www.openssh.com/txt/release-7.1p2`
`URL:https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a78`
`↪9277bb0733ca36e1c0`

Medium (CVSS: 4.3)
NVT: OpenSSH Security Bypass Vulnerability

Product detection result
`cpe:/a:openbsd:openssh:4.4`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is running OpenSSH and is prone to security bypass vulnerability.

Vulnerability Detection Result
`Installed version: 4.4`
`Fixed version: 6.9`

Impact
Successful exploitation will allow remote attackers to bypass intended access restrictions.
Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to OpenSSH version 6.9 or later. For updates refer to http://www.openssh.com

Affected Software/OS
OpenSSH versions before 6.9

Vulnerability Insight
The flaw is due to the refusal deadline was not checked within the x11_open_helper function.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`OpenSSH Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.806049
Version used: `$Revision: 4336 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:4.4`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2015-5352`
`Other:`
`URL:http://openwall.com/lists/oss-security/2015/07/01/10`

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result
```
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
3des-cbc
```

... continues on next page ...

... continued from previous page ...

```
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution
Solution type: Mitigation
Disable the weak encryption algorithms.

Vulnerability Insight
The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details:`SSH Weak Encryption Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `$Revision: 4490 $`

References
```
Other:
  URL:https://tools.ietf.org/html/rfc4253#section-6.3
   URL:https://www.kb.cert.org/vuls/id/958563
```

[return to 192.168.27.45]

2.1.6 Medium 631/tcp

Medium (CVSS: 6.5)
NVT: CUPS < 1.1.23 Multiple Vulnerabilities

Product detection result
```
cpe:/a:apple:cups:1.1
Detected by CUPS Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900348)
```

... continues on next page ...

... continued from previous page ...

Summary
The remote host is running a CUPS server whose version number is between 1.0.4 and 1.1.22 inclusive. Such versions are prone to multiple vulnerabilities :
- The is_path_absolute function in scheduler/client.c for the daemon in CUPS allows remote attackers to cause a denial of service (CPU consumption by tight loop) via a '..\..' URL in an HTTP request.
- A remotely exploitable buffer overflow in the 'hpgltops' filter that enable specially crafted HPGL files can execute arbitrary commands as the CUPS 'lp' account.
- A local user may be able to prevent anyone from changing his or her password until a temporary copy of the new password file is cleaned up ('lppasswd' flaw).
- A local user may be able to add arbitrary content to the password file by closing the stderr file descriptor while running lppasswd (lppasswd flaw).
- A local attacker may be able to truncate the CUPS password file, thereby denying service to valid clients using digest authentication. (lppasswd flaw).
- The application applys ACLs to incoming print jobs in a case-sensitive fashion. Thus, an attacker can bypass restrictions by changing the case in printer names when submitting jobs. [Fixed in 1.1.21.]

Vulnerability Detection Result
`Installed version: 1.1`
`Fixed version: 1.1.23`

Solution
Solution type: VendorFix
Upgrade to CUPS 1.1.23 or later.

Vulnerability Detection Method
Details:`CUPS < 1.1.23 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.16141
Version used: `$Revision: 6040 $`

Product Detection Result
Product: `cpe:/a:apple:cups:1.1`
Method: `CUPS Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900348)

References
`CVE: CVE-2004-1267, CVE-2004-1268, CVE-2004-1269, CVE-2004-1270, CVE-2005-2874`
`BID:11968, 12004, 12005, 12007, 12200, 14265`
`Other:`
`OSVDB:12439`
`OSVDB:12453`
`OSVDB:12454`
`FLSA:FEDORA-2004-908`
`FLSA:FEDORA-2004-559`

... continues on next page ...

... continued from previous page ...

FLSA:FEDORA-2004-560
GLSA:GLSA-200412-25
URL:http://www.cups.org/str.php?L700
URL:http://www.cups.org/str.php?L1024
URL:http://www.cups.org/str.php?L1023
URL:http://www.cups.org/str.php?L1042

[return to 192.168.27.45]

2.1.7 Medium 80/tcp

Medium (CVSS: 4.3)
NVT: 12Planet Chat Server one2planet.infolet.InfoServlet XSS

Summary
The remote host contains the 12Planet Chat Server CGI which is vulnerable to a cross-site scripting issue.
There is a bug in this software which makes it vulnerable to cross site scripting attacks.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45/info/servlet/one2planet.infolet.InfoServlet
↪?page=<script>foo</script>

Impact
An attacker may use this bug to steal the credentials of the legitimate users of this site.

Solution
Solution type: VendorFix
Upgrade to the newest version of this software

Vulnerability Detection Method
Details:12Planet Chat Server one2planet.infolet.InfoServlet XSS
OID:1.3.6.1.4.1.25623.1.0.12299
Version used: $Revision: 6046 $

References
CVE: CVE-2004-0678
BID:10659

Medium (CVSS: 4.9)
NVT: Apache 'Options' and 'AllowOverride' Directives Security Bypass Vulnerability

Summary
Apache HTTP server is prone to a security-bypass vulnerability related to the handling of specific configuration directives.

... continues on next page ...

... continued from previous page ...

A local attacker may exploit this issue to execute arbitrary code within the context of the webserver process. This may result in elevated privileges or aid in further attacks.
Versions prior to Apache 2.2.9 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see http://httpd.apache.org/ for more Information.

Vulnerability Detection Method
Details:`Apache 'Options' and 'AllowOverride' Directives Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100211
Version used: `$Revision: 4574 $`

References
`CVE: CVE-2009-1195`
`BID:35115`
`Other:`
`URL:http://www.securityfocus.com/bid/35115`

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary
This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Apache HTTP Server version 2.2.22 or later, For updates refer to http://httpd.apache.org/

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method
Details:Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: $Revision: 5950 $

References
CVE: CVE-2012-0053
BID:51706
Other:
URL:http://secunia.com/advisories/47779
URL:http://www.exploit-db.com/exploits/18442
URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
URL:http://httpd.apache.org/security/vulnerabilities_22.html
URL:http://svn.apache.org/viewvc?view=revision&revision=1235454
URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l

Medium (CVSS: 5.1)
NVT: Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Linux)

Product detection result
cpe:/a:apache:http_server:1.3.37
Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004
↪98)

Summary
This host is installed with Apache HTTP Server and is prone to man-in-the-middle attack vulnerability.

Vulnerability Detection Result
Installed version: 1.3.37
Fixed version: 2.4.24

Impact
Successful exploitation will allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted proxy header in an HTTP request.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 2.4.24, or 2.2.32, or newer. For updates refer http://www.apache.org

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Apache HTTP Server through 2.4.23 on Linux —- NOTE: Apache HTTP Server 2.2.32 is not vulnerable —-

Vulnerability Insight
The flaw is due to 'CGI Servlet' does not protect applications from the presence of untrusted client data in the 'HTTP_PROXY' environment variable.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808632
Version used: `$Revision: 5588 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:1.3.37`
Method: `Apache Web Server Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
`CVE: CVE-2016-5387`
`BID:91816`
`Other:`
`URL:https://www.apache.org/security/asf-httpoxy-response.txt`

Medium (CVSS: 5.0)
NVT: Apache HTTP Server Mod_Lua Denial of service Vulnerability -01 May15

Product detection result
`cpe:/a:apache:http_server:1.3.37`
`Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.9004`
`↪98)`

Summary
This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 1.3.37`
`Fixed version: 2.4.13`

Impact
Successful exploitation will allow a remote attackers to cause a denial of service via some crafted dimension.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to version 2.4.13 or later, For updates refer http://www.apache.org

Affected Software/OS
Apache HTTP Server versions through 2.4.12.

Vulnerability Insight
Flaw is due to vulnerability in lua_websocket_read function in lua_request.c in the mod_lua module.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`Apache HTTP Server Mod_Lua Denial of service Vulnerability -01 May15`
OID:1.3.6.1.4.1.25623.1.0.805616
Version used: `$Revision: 3496 $`

Product Detection Result
Product: `cpe:/a:apache:http_server:1.3.37`
Method: `Apache Web Server Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References
`CVE: CVE-2015-0228`
`BID:73041`
`Other:`
`URL:https://bugs.mageia.org/show_bug.cgi?id=15428`
`URL:http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHANGES`

Medium (CVSS: 5.0)
NVT: Apache mod_proxy_ajp Information Disclosure Vulnerability

Summary
This host is running Apache Web Server and is prone to Information Disclosure Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let the attacker craft a special HTTP POST request and gain sensitive information about the web server.
Impact level: Application

Solution

... continues on next page ...

... continued from previous page ...

Upgrade to Apache HTTP Version 2.2.15 or later For further updates refer, http://httpd.apache.org/download.cgi

Affected Software/OS
Apache HTTP Version 2.2.11
Workaround: Update mod_proxy_ajp.c through SVN Repository (Revision 767089) http://www.apache.org/dist/httpd/patches/apply_to_2.2.11/PR46949.diff

Vulnerability Insight
This flaw is due to an error in 'mod_proxy_ajp' when handling improperly malformed POST requests.

Vulnerability Detection Method
Details:Apache mod_proxy_ajp Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900499
Version used: $Revision: 5055 $

References
CVE: CVE-2009-1191
BID:34663
Other:
URL:http://secunia.com/advisories/34827
URL:http://xforce.iss.net/xforce/xfdb/50059
URL:http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=766938&r2=76708
↪9

Medium (CVSS: 4.6)
NVT: Apache Web Server Configuration File Environment Variable Local Buffer Overflow Vulnerability

Summary
According to its version number, the remote version of Apache Web Server is prone to a local buffer-overflow vulnerability that affects a configuration file environment variable. This occurs because the application fails to validate user-supplied string lengths before copying them into finite process buffers.
An attacker may leverage this issue to execute arbitrary code on the affected computer with the privileges of the Apache webserver process.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
The vendor has released an upgrade. Please see http://www.apache.org/dist/httpd/Announcement2.html for more information.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details:Apache Web Server Configuration File Environment Variable Local Buffer Overflow.
↪..
OID:1.3.6.1.4.1.25623.1.0.100172
Version used: $Revision: 4574 $

References
CVE: CVE-2004-0747
BID:11182
Other:
URL:http://www.securityfocus.com/bid/11182

Medium (CVSS: 5.0)
NVT: Apache Web Server Linefeed Memory Allocation Denial Of Service Vulnerability

Summary
Apache 2.0 series webservers are prone to a denial-of-service condition. This issue occurs because of the way that Apache handles excessive amounts of consecutive linefeed characters. The server may allocate large amounts of memory, resulting in a denial of service.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
This vulnerability does not affect Apache 2.0.45. Users are advised to upgrade.

Vulnerability Detection Method
Details:Apache Web Server Linefeed Memory Allocation Denial Of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100171
Version used: $Revision: 4574 $

References
CVE: CVE-2003-0132
BID:7254
Other:
URL:http://www.securityfocus.com/bid/7254
URL:http://httpd.apache.org/

Medium (CVSS: 4.3)
NVT: Basit cms Cross Site Scripting Bugs

Summary
The remote web server contains a PHP script which is vulnerable to a cross site scripting and SQL injection issue.
Description :

... continues on next page ...

... continued from previous page ...

Basit cms 1.0 has a cross site scripting bug. An attacker may use it to perform a cross site scripting attack on this host.
In addition to this, it is vulnerable to a SQL insertion attack which may allow an attacker to get the control of your database.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/modules/Submit/index.php?op=pre&title=`
`↪<script>window.alert(document.cookie);</script>`

Solution
Upgrade to a newer version.

Vulnerability Detection Method
Details:`Basit cms Cross Site Scripting Bugs`
OID:1.3.6.1.4.1.25623.1.0.11445
Version used: `$Revision: 5781 $`

References
`BID:7139`

Medium (CVSS: 4.3)
NVT: BLOG:CMS Multiple Cross Site Scripting Vulnerabilities

Summary
BLOG:CMS is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/photo/templates/admin_default/confirm.`
`↪tpl.php?nsextt="><script>alert(/openvas-xss-test/);</script>`

Impact
An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker steal cookie-based authentication credentials and launch other attacks.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
BLOG:CMS 4.2.1.f is vulnerable other versions may also be affected.

Vulnerability Detection Method
Details:`BLOG:CMS Multiple Cross Site Scripting Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.103178

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 3983 $

References

BID:48132
Other:
URL:http://www.securityfocus.com/bid/48132
URL:http://blogcms.com/
URL:http://www.rul3z.de/advisories/SSCHADV2011-007.txt

Medium (CVSS: 4.3)
NVT: CGIEmail's Cross Site Scripting Vulnerability (cgicso)

Summary

The remote web server contains the 'CGIEmail' CGI, a web based form to send emails which is vulnerable to a cross site scripting vulnerability.
The remote version of this software contains a vulnerability caused by inadequate processing of queries by CGIEmail's cgicso that results in a cross site scripting condition.

Vulnerability Detection Result

Vulnerable url: http://192.168.27.45/info/cgicso?query=<script>alert('foo')</scr
↪ipt>

Solution

Modify cgilib.c to contain a stripper function that will remove any HTML or JavaScript tags.

Vulnerability Detection Method

Details:CGIEmail's Cross Site Scripting Vulnerability (cgicso)
OID:1.3.6.1.4.1.25623.1.0.10780
Version used: $Revision: 6056 $

Medium (CVSS: 4.3)
NVT: DCP-Portal XSS

Summary

You are running a version of DCP-Portal which is older or equals to v5.3.2
This version is vulnerable to:
- Cross-site scripting flaws in calendar.php script, which may let an attacker to execute arbitrary code in the browser of a legitimate user.
In addition to this, your version may also be vulnerable to:
- HTML injection flaws, which may let an attacker to inject hostile HTML and script code that could permit cookie-based credentials to be stolen and other attacks.
- HTTP response splitting flaw, which may let an attacker to influence or misrepresent how web content is served, cached or interpreted.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerable url: http://192.168.27.45/info/calendar.php?year=2004&month=<script>f
↪oo</script>&day=01

Solution
Solution type: VendorFix
Upgrade to a newer version when available

Vulnerability Detection Method
Details:DCP-Portal XSS
OID:1.3.6.1.4.1.25623.1.0.11446
Version used: $Revision: 6053 $

References
CVE: CVE-2004-2511, CVE-2004-2512
BID:7141, 7144, 11338, 11339, 11340
Other:
OSVDB:10585
OSVDB:10586
OSVDB:10587
OSVDB:10588
OSVDB:10589
OSVDB:10590
OSVDB:11405
URL:http://archives.neohapsis.com/archives/bugtraq/2004-10/0042.html
URL:http://archives.neohapsis.com/archives/fulldisclosure/2004-10/0131.html

Medium (CVSS: 4.3)
NVT: DHCart Multiple Cross Site Scripting And HTML Injection Vulnerabilities

Summary
DHCart is prone to multiple cross-site scripting and HTML-injection vulnerabilities because it fails to sufficiently sanitize user-supplied data.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45/info/order.php?dhaction=check&submit_domain
↪=Register&domain=<script>alert(document.cookie);</script>&ext1=on

Impact
Attacker-supplied HTML or JavaScript code could run in the context of the affected site, potentially allowing the attacker to steal cookie-based authentication credentials and to control how the site is rendered to the user other attacks are also possible.

Solution
Solution type: VendorFix
Update DHCart to version 3.88 or newer.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
DHCart 3.84 is vulnerable other versions may also be affected.

Vulnerability Detection Method
Details:DHCart Multiple Cross Site Scripting And HTML Injection Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100028
Version used: $Revision: 4655 $

References
CVE: CVE-2008-6297
BID:32117

Medium (CVSS: 5.0)
NVT: Enabled Directory Listing Detection

Summary
The script attempts to identify directories with an enabled directory listing.

Vulnerability Detection Result
The following directories with an enabled directory listing were identified:
http://192.168.27.45/
http://192.168.27.45/beef
http://192.168.27.45/beef/include
http://192.168.27.45/beef/modules
http://192.168.27.45/beef/tmp
http://192.168.27.45/beef/tmp/de2dfc7a9a4bfd754ffd38a21373c091
http://192.168.27.45/manual/howto
http://192.168.27.45/olate/templates/olate
http://192.168.27.45/olate/templates/olate/global
http://192.168.27.45/webexploitation_package_01
http://192.168.27.45/webexploitation_package_02
http://192.168.27.45/webexploitation_package_02/board51
http://192.168.27.45/webexploitation_package_02/board51/boarddata
http://192.168.27.45/webexploitation_package_02/board51/solution
http://192.168.27.45/webexploitation_package_02/iseasynews
http://192.168.27.45/webexploitation_package_02/isguestbook/smileys
http://192.168.27.45/webexploitation_package_02/isshout/smileys
http://192.168.27.45/webexploitation_package_02/isshout/templates/default/
http://192.168.27.45/webexploitation_package_02/nabopoll
http://192.168.27.45/webexploitation_package_02/nabopoll/includes
http://192.168.27.45/webexploitation_package_02/nabopoll/templates
http://192.168.27.45/webexploitation_package_02/nabopoll/test
http://192.168.27.45/webexploitation_package_02/solutions
http://192.168.27.45/webexploitation_package_02/webnews/design
Please review the content manually.

Impact

... continues on next page ...

... continued from previous page ...

Based on the information shown an attacker might be able to gather additional info about the structure of this application.

Solution
Solution type: Mitigation
If not needed disable the directory listing within the webservers config.

Affected Software/OS
Webservers with an enabled directory listing.

Vulnerability Detection Method
Check the detected directories if a directory listing is enabled.
Details:`Enabled Directory Listing Detection`
OID:1.3.6.1.4.1.25623.1.0.111074
Version used: `$Revision: 5440 $`

References
```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_
↪Directory_Indexing
```

Medium (CVSS: 5.0)
NVT: Faq-O-Matic fom.cgi XSS

Summary
The remote host runs Faq-O-Matic, a CGI-based system that automates the process of maintaining a FAQ.
The remote version of this software is vulnerable to cross-site scripting attacks in the script 'fom.cgi'.

Vulnerability Detection Result
```
Vulnerable url: http://192.168.27.45/info/fom.cgi?cmd=<script>foo</script>&file=
↪1&keywords=openvas
```

Impact
With a specially crafted URL, an attacker can cause arbitrary code execution resulting in a loss of integrity.

Solution
Solution type: VendorFix
Upgrade to the latest version of this software

Vulnerability Detection Method
Details:`Faq-O-Matic fom.cgi XSS`
OID:1.3.6.1.4.1.25623.1.0.15540
Version used: `$Revision: 6053 $`

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2002-0230, CVE-2002-2011
BID:4565

Medium (CVSS: 4.3)
NVT: Goollery Multiple XSS

Summary
Goollery, a GMail based photo gallery written in PHP, is installed on this remote host.
According to it's version number, this host is vulnerable to multiple cross-site-scripting (XSS) attacks eg, through the 'viewpic.php' script. An attacker, exploiting these flaws, would need to be able to coerce a user to browse a malicious URI. Upon successful exploitation, the attacker would be able to run code within the web-browser in the security context of the remote server.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45/info/viewpic.php?id=7&conversation_id=<scri
↪pt>foo</script>&btopage=0

Solution
Upgrade to Goollery 0.04b or newer.

Vulnerability Detection Method
Details:Goollery Multiple XSS
OID:1.3.6.1.4.1.25623.1.0.15717
Version used: $Revision: 5781 $

References
CVE: CVE-2004-2245
BID:11587
Other:
OSVDB:11318
OSVDB:11319
OSVDB:11320
OSVDB:11624

Medium (CVSS: 5.8)
NVT: http TRACE XSS attack

Summary
Debugging functions are enabled on the remote HTTP server.
The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

... continues on next page ...

... continued from previous page ...

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Vulnerability Detection Result

```
Solution:
Add the following lines for each virtual host in your configuration file :
    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]
See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
```

Solution
Disable these methods.

Vulnerability Detection Method
Details:`http TRACE XSS attack`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `$Revision: 6063 $`

References

```
CVE: CVE-2004-2320, CVE-2003-1567
BID:9506, 9561, 11604
Other:
  URL:http://www.kb.cert.org/vuls/id/867593
```

Medium (CVSS: 6.4)
NVT: ionCube Loader Wizard 'loader-wizard.php' Multiple Security Vulnerabilities

Summary
ionCube Loader is prone to multiple security vulnerabilities:

Vulnerability Detection Result

```
Vulnerable url: http://192.168.27.45/info/loader-wizard.php?page=phpinfo
```

Impact
ionCube Loader is prone to the following security vulnerabilities: 1. A cross-site scripting vulnerbility 2. An information-disclosure vulnerabilities 3. An Arbitrary File Disclosure Vulnerability

Solution
Updates are available.

Affected Software/OS
Versions prior to ionCube Loader 2.46 are vulnerable.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
An attacker can exploit these issues to obtain potentially sensitive information, to view arbitrary files from the local filesystem and to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials to launch other attacks.

Vulnerability Detection Method
Send a crafted HTTP GET request and check the response.
Details:`ionCube Loader Wizard 'loader-wizard.php' Multiple Security Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.103932
Version used: `$Revision: 5698 $`

References
`BID:66531`
`Other:`
`URL:http://www.securityfocus.com/bid/66531`

Medium (CVSS: 4.3)
NVT: JShop Cross-Site Scripting Vulnerability

Summary
The remote host is running J-Shop, an e-Commerce suite written in PHP.
The remote version of this software is vulnerable to a cross-site scripting attack. An attacker can exploit it by compromising the parameters to the files help.php and/or search.php.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/page.php?xPage=<script>alert(document.`
`↪cookie)</script>`

Impact
This can be used to take advantage of the trust between a client and server allowing the malicious user to execute malicious JavaScript on the client's machine.

Solution
Solution type: VendorFix
Upgrade to the latest version of this software

Vulnerability Detection Method
Details:`JShop Cross-Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.14352
Version used: `$Revision: 6053 $`

References
`CVE: CVE-2004-2084`
`BID:12403, 11003, 9609`

Medium (CVSS: 4.3)
NVT: Multiple Cross Site Scripting and SQL Injection vulnerabilities in XRMS

Summary
XRMS is a web-based application for managing business entities such as employees, customers, contacts, activities. The application is vulnerable to simple Cross Site Scripting, which can be used for several isues.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/login.php?target=test<script>alert('at`
`↪tack');</script>`

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Vulnerability Detection Method
Details:`Multiple Cross Site Scripting and SQL Injection vulnerabilities in XRMS`
OID:1.3.6.1.4.1.25623.1.0.101008
Version used: `$Revision: 5231 $`

References
`CVE: CVE-2008-3664`

Medium (CVSS: 4.3)
NVT: My Little Forum XSS Vulnerability

Summary
The remote host is running 'My Little Forum', a free CGI suite to manage discussion forums. This PHP/MySQL based forum suffers from a Cross Site Scripting vulnerability. This can be exploited by including arbitrary HTML or even JavaScript code in the parameters (forum_contact, category and page), which will be executed in user's browser session when viewed.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/email.php?forum_contact="><script>foo<`
`↪/script>`

Vulnerability Detection Method
Details:`My Little Forum XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.11960
Version used: `$Revision: 6053 $`

References
`BID:9286`
`Other:`

. . . continues on next page . . .

... continued from previous page ...

URL:http://secunia.com/advisories/10489/
URL:http://xforce.iss.net/xforce/xfdb/14066
URL:http://www.securitytracker.com/id/1008545
URL:http://www.os2world.com/content/view/12704/79/

Medium (CVSS: 5.8)
NVT: Nuked-klan Cross Site Scripting Bugs

Summary
Nuked-klan 1.3b has a cross site scripting bug. An attacker may use it to perform a cross site scripting attack on this host.
In addition to this, another flaw may allow an attacker to obtain the physical path of the remote CGI directory.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45/beef/hook/index.php?file=Liens&op="><script
↪>window.alert('test');</script>

Solution
Solution type: VendorFix
Upgrade to a newer version.

Vulnerability Detection Method
Details:Nuked-klan Cross Site Scripting Bugs
OID:1.3.6.1.4.1.25623.1.0.11447
Version used: $Revision: 6056 $

References
CVE: CVE-2003-1238
BID:6916, 6917

Medium (CVSS: 5.0)
NVT: PHP 'extract()' Function Security Bypass Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is running PHP and is prone to security bypass vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4

... continues on next page ...

... continued from previous page ...

Fixed version: 5.2.15

Impact
Successful exploitation could allows remote attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input.
Impact Level: Network

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.15 or later For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.2.15

Vulnerability Insight
The flaw is due to error in 'extract()' function, it does not prevent use of the 'EXTR_OVERWRITE' parameter to overwrite the GLOBALS superglobal array.

Vulnerability Detection Method
Details:PHP 'extract()' Function Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801731
Version used: $Revision: 4502 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2011-0752
Other:
URL:http://www.php.net/releases/5_2_15.php
URL:http://www.openwall.com/lists/oss-security/2010/12/13/4

Medium (CVSS: 6.4)
NVT: PHP 'make_http_soap_request' Information Disclosure Vulnerability (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with PHP and is prone to denial of service or information disclosure vulnerabilities

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.4.44`

Impact
Successfully exploiting this issue allow remote attackers to obtain sensitive information from process memory or cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or 7.0.4, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 on Linux

Vulnerability Insight
The flaw is due an error in the 'make_http_soap_request' function in 'ext/soap/php_http.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP 'make_http_soap_request' Information Disclosure Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808666
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-3185`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:http://www.php.net/ChangeLog-7.php`

Medium (CVSS: 5.0)
NVT: PHP 'unserialize()' Function Denial of Service Vulnerability

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
The host is running PHP and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: N/A

Impact
Successful exploitation could allow attackers to execute arbitrary PHP code and cause denial of service.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
PHP 5.3.0 and prior on all running platform.

Vulnerability Insight
An error in 'unserialize()' function while processing malformed user supplied data containing a long serialized string passed via the '__wakeup()' or '__destruct()' methods.

Vulnerability Detection Method
Details:PHP 'unserialize()' Function Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900993
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-4418
Other:
URL:http://www.security-database.com/detail.php?alert=CVE-2009-4418
URL:http://www.suspekt.org/downloads/POC2009-ShockingNewsInPHPExploitation.pd

... continues on next page ...

... continued from previous page ...

↪f

Medium (CVSS: 5.0)
NVT: PHP 5.2.8 and Prior Versions Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to multiple security vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.9

Impact
Successful exploits could allow an attacker to cause a denial-of-service condition. An unspecified issue with an unknown impact was also reported.

Solution
Solution type: VendorFix
The vendor has released PHP 5.2.9 to address these issues. Please see http://www.php.net/ fore more information.

Affected Software/OS
These issues affect PHP 5.2.8 and prior versions.

Vulnerability Detection Method
Details:PHP 5.2.8 and Prior Versions Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100146
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-1271
BID:33927
Other:
URL:http://www.securityfocus.com/bid/33927

Medium (CVSS: 4.3)
NVT: PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)`

Summary
This host is installed with PHP and is prone to cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.4.38`

Impact
Successfully exploiting this issue allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging '%0A%20' or '%0D%0A%20' mishandling in the header function.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.4.38, or 5.5.22, or 5.6.6, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 on Linux

Vulnerability Insight
The flaw is due to the 'sapi_header_op' function in 'main/SAPI.c' script supports deprecated line folding without considering browser compatibility.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.809137
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2015-8935`

. . . continues on next page . . .

... continued from previous page ...

BID:92356
Other:
URL:https://bugs.php.net/bug.php?id=68978

Medium (CVSS: 6.4)
NVT: PHP dba_replace Denial of Service Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
The host is running PHP and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.7

Impact
Successful exploitation could allow attackers to execute arbitrary code corrupt files and cause denial of service.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.7 or later, http://www.php.net/downloads.php

Affected Software/OS
PHP 4.x and 5.2.6 on all running platform.

Vulnerability Insight
An error occurs in 'dba_replace()' function while processing malformed user supplied data containing a key with the NULL byte.

Vulnerability Detection Method
Details:PHP dba_replace Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900925
Version used: $Revision: 4505 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2008-7068
BID:33498
Other:
URL:http://xforce.iss.net/xforce/xfdb/47316
URL:http://www.securityfocus.com/archive/1/archive/1/498746/100/0/threaded

Medium (CVSS: 6.8)
NVT: PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.18

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.18, or 7.0.3, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.18 and 7.x before 7.0.3 on Linux

Vulnerability Insight
The flaw is due an improper handling of zero-size './/@LongLink' files by 'phar_make_dirstream' function in ext/phar/dirstream.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808609
Version used: $Revision: 5083 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-4343
BID:89179
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.openwall.com/lists/oss-security/2016/04/28/2

Medium (CVSS: 6.4)
NVT: PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.31

Impact
Successfully exploiting this issue allow attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 on Linux.

Vulnerability Insight
The flaw is due to the 'sapi/fpm/fpm/fpm_log.c' script misinterprets the semantics of the snprintf return value.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.809139
Version used: $Revision: 5083 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2016-5114
BID:81808
Other:
URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 5.0)
NVT: PHP Denial Of Service Vulnerability - April09

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
The host is installed with PHP and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.10

Impact
Successful exploitation could result in denial of service condition.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.2.9 or above, http://www.php.net/downloads.php
Workaround: For workaround refer below link, http://cvs.php.net/viewvc.cgi/php-src/ext/json/JSON_parser.c?r1=1.1.2.14&r2=1.1.2.15

Affected Software/OS
PHP version prior to 5.2.9

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Improper handling of .zip file while doing extraction via php_zip_make_relative_path function in php_zip.c file.

Vulnerability Detection Method
Details:PHP Denial Of Service Vulnerability - April09
OID:1.3.6.1.4.1.25623.1.0.800393
Version used: $Revision: 4504 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-1272
Other:
URL:http://www.php.net/releases/5_2_9.php
URL:http://www.openwall.com/lists/oss-security/2009/04/01/9

Medium (CVSS: 5.0)
NVT: PHP FastCGI Module File Extension Denial Of Service Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP is prone to a denial-of-service vulnerability because the application fails to handle certain file requests.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.9

Impact
Attackers can exploit this issue to crash the affected application, denying service to legitimate users.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP 4.4 prior to 4.4.9 and PHP 5.2 through 5.2.6 are vulnerable.

Vulnerability Detection Method
Details:PHP FastCGI Module File Extension Denial Of Service Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100582
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-3660
BID:31612
Other:
URL:http://www.securityfocus.com/bid/31612
URL:http://www.openwall.com/lists/oss-security/2008/08/08/2
URL:http://www.php.net/ChangeLog-5.php#5.2.8
URL:http://www.php.net
URL:http://support.avaya.com/elmodocs2/security/ASA-2009-161.htm

Medium (CVSS: 5.0)
NVT: PHP Fileinfo Component Denial of Service Vulnerability (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.0

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service.
Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to PHP version 5.6.0 For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.0 on Linux

Vulnerability Insight
The flaw is due an improper validation of input to zero root_storage value in a CDF file.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Fileinfo Component Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808669
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2014-0236`
`BID:90957`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

Medium (CVSS: 5.1)
NVT: PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
This host is installed with PHP and is prone to Man-in-the-middle attack vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.6.24/7.0.9`

Impact
Successfully exploiting this issue may allow remote, unauthenticated to conduct MITM attacks on internal server subrequests or direct the server to initiate connections to arbitrary hosts or to cause a denial of service.

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution
Solution type: VendorFix
Update to PHP version 5.6.24 or 7.0.19. For updates refer to http://www.php.net

Affected Software/OS
PHP versions 5.x through 5.6.23 and 7.0.x through 7.0.8 on Linux

Vulnerability Insight
The web servers running in a CGI or CGI-like context may assign client request Proxy header values to internal HTTP_PROXY environment variables and 'HTTP_PROXY' is improperly trusted by some PHP libraries and applications and flaw exist in the gdImageCropThreshold function in 'gd_crop.c' in the GD Graphics Library.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808628
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2016-5385, CVE-2016-6128`
`BID:91821, 91509`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`
`URL:http://www.php.net/ChangeLog-7.php`
`URL:http://www.kb.cert.org/vuls/id/797896`
`URL:https://bugs.php.net/bug.php?id=72573`
`URL:https://bugs.php.net/bug.php?id=72494`

Medium (CVSS: 5.0)
NVT: PHP Multiple Denial of Service Vulnerabilities (Linux)

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary

... continues on next page ...

... continued from previous page ...

This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.6.12`

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (application crash or memory consuption).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.12 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.6.12 on Linux

Vulnerability Insight
Multiple flaws are due to - An improper handling of driver behavior for SQL_WVARCHAR columns in the 'odbc_bindcols function' in 'ext/odbc/php_odbc.c' script. - The 'gdImageScaleTwoPass' function in gd_interpolation.c script in the GD Graphics Library uses inconsistent allocate and free approaches.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Multiple Denial of Service Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808611
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2015-8877, CVE-2015-8879, CVE-2015-8874`
`BID:90866, 90842, 90714`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

Medium (CVSS: 6.8)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed Version: 4.4.4
Fixed Version: 5.5.30

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP 5.5.30 or 5.6.14 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.30 and 5.6.x before 5.6.14

Vulnerability Insight
Multiple flaws are due to, - An Off-by-one error in the 'phar_parse_zipfile' function within ext/phar/zip.c script. - An error in the 'phar_get_entry_data' function in ext/phar/util.c script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.806649
Version used: $Revision: 5082 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2015-7804, CVE-2015-7803
BID:76959
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:https://bugs.php.net/bug.php?id=70433

... continues on next page ...

... continued from previous page ...

URL:http://www.openwall.com/lists/oss-security/2015/10/05/8

Medium (CVSS: 5.0)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.6.30

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer over-read or application crash).
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.6.30, 7.0.15, 7.1.1 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1.

Vulnerability Insight
Multiple flaws are due to - The exif_convert_any_to_int function in ext/exif/exif.c tries to divide the minimum representable negative integer by -1.
- A mishandled serialized data in a finish_nested_data call within the object_common1 function in ext/standard/var_unserializer.c.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check if the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Linux)
OID:1.3.6.1.4.1.25623.1.0.108052
Version used: $Revision: 5099 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.103592)

References

```
CVE: CVE-2016-10161, CVE-2016-10158
Other:
  URL:http://www.php.net/ChangeLog-5.php
   URL:http://www.php.net/ChangeLog-7.php
```

Medium (CVSS: 5.0)
NVT: PHP Multiple Security Bypass Vulnerabilities

Product detection result

```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary

This host is running PHP and is prone to multiple security bypass vulnerability.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     5.3.4
```

Impact

Successful exploitation could allow remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact.
Impact Level: Application/Network

Solution

Solution type: VendorFix
Upgrade to PHP 5.3.4 or later For updates refer to http://www.php.net/downloads.php

Affected Software/OS

PHP version prior to 5.3.4

Vulnerability Insight

The flaws are caused to: - An error in handling pathname which accepts the '?' character in a pathname. - An error in 'iconv_mime_decode_headers()' function in the 'Iconv' extension. - 'SplFileInfo::getType' function in the Standard PHP Library (SPL) extension, does not properly detect symbolic links in windows. - Integer overflow in the 'mt_rand' function. - Race condition in the 'PCNTL extension', when a user-defined signal handler exists.

Vulnerability Detection Method

Details:`PHP Multiple Security Bypass Vulnerabilities`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.801585
Version used: $Revision: 4502 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2006-7243, CVE-2010-4699, CVE-2011-0754, CVE-2011-0753, CVE-2011-0755
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:http://www.php.net/releases/5_3_4.php
URL:http://openwall.com/lists/oss-security/2010/12/09/9
URL:http://svn.php.net/viewvc?view=revision&revision=305507

Medium (CVSS: 6.4)
NVT: PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
This host is installed with PHP and is prone to out-of-bounds read memory corruption vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.5.31

Impact
Successfully exploiting this issue allow remote attackers to obtain sensitive information or cause a denial-of-service condition.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 on Linux

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw is due to memory corruption vulnerability via a large 'bgd_color' argument to the 'imagerotate' function in 'ext/gd/libgd/gd_interpolation.c' script.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.807504
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2016-1903
BID:79916
Other:
  URL:https://bugs.php.net/bug.php?id=70976
   URL:http://www.openwall.com/lists/oss-security/2016/01/14/8
```

Medium (CVSS: 5.1)
NVT: PHP Ovrimos Extension Code Execution Vulnerability

Product detection result
```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary
PHP is prone to a code-execution vulnerability due to a design error in a vulnerable extension.

Vulnerability Detection Result
```
Installed version: 4.4.4
Fixed version:     4.4.5
```

Impact
Successful exploits may allow an attacker to execute arbitrary code in the context of the affected application. Failed exploits would likely crash PHP.

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Affected Software/OS
PHP versions prior to 4.4.5 or 5.2.1 with a compiled 'Ovrimos SQL Server Extension' are vulnerable to this issue.

Vulnerability Insight
For this vulnerability to occur, the non-maintained 'Ovrimos SQL Server Extension' must have been compiled into the targeted PHP implementation.

Vulnerability Detection Method
Details:`PHP Ovrimos Extension Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100604
Version used: `$Revision: 4503 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
```
CVE: CVE-2007-1379, CVE-2007-1378
BID:22833
Other:
  URL:http://www.securityfocus.com/bid/22833
   URL:http://www.php.net
   URL:http://www.php-security.org/MOPB/MOPB-13-2007.html
```

Medium (CVSS: 5.0)
NVT: PHP PHP_Binary Heap Information Leak Vulnerability

Product detection result
```
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)
```

Summary
PHP 'php_binary' serialization handler is prone to a heap- information leak.

Vulnerability Detection Result
```
Installed version: 4.4.4
Fixed version:     4.4.5
```

Impact

... continues on next page ...

... continued from previous page ...

A local attacker can exploit this issue to obtain sensitive information (such as heap offsets and canaries) that may aid in other attacks.

Solution
Solution type: VendorFix
The vulnerability arises because of a missing boundary check in the extraction of variable names.

Affected Software/OS
PHP4 versions prior to 4.4.5 PHP5 versions prior to 5.2.1

Vulnerability Insight
The vulnerability arises because of a missing boundary check in the extraction of variable names.

Vulnerability Detection Method
Details:`PHP PHP_Binary Heap Information Leak Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100603
Version used: `$Revision: 4503 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2007-1380`
`BID:22805`
`Other:`
`URL:http://www.securityfocus.com/bid/22805`
`URL:http://www8.itrc.hp.com/service/cki/docDisplay.do?docId=c01056506`
`URL:http://www.php.net`
`URL:http://lists.suse.com/archive/suse-security-announce/2007-May/0007.html`

Medium (CVSS: 6.8)
NVT: PHP Printf() Function 64bit Casting Multiple Format String Vulnerabilities

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
PHP is prone to multiple format-string vulnerabilities due to a design error when casting 64-bit variables to 32 bits.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 4.4.5

Impact
Attackers may be able to exploit these issues to execute arbitrary code in the context of the webserver process or to cause denial-of-service conditions.

Solution
Solution type: VendorFix
The vendor released versions 5.2.1 and 4.4.5 to address these issues. Please see the references for more information.

Affected Software/OS
These issues affect PHP versions prior to 4.4.5 and 5.2.1 running on 64-bit computers.

Vulnerability Detection Method
Details:PHP Printf() Function 64bit Casting Multiple Format String Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100595
Version used: $Revision: 4503 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1884
BID:23219
Other:
URL:http://www.securityfocus.com/bid/23219
URL:http://www8.itrc.hp.com/service/cki/docDisplay.do?docId=c01056506
URL:http://www.php-security.org/MOPB/MOPB-38-2007.html
URL:http://www.php.net/releases/4_4_5.php
URL:http://www.php.net/releases/5_2_1.php
URL:http://www.php.net

Medium (CVSS: 4.3)
NVT: PHP SOAP Parser Multiple Information Disclosure Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

... continues on next page ...

... continued from previous page ...

Summary
This host is installed with PHP and is prone to multiple information disclosure vulnerabilities.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.3.22/5.4.12`

Impact
Successful exploitation will allow remote attackers to obtain sensitive information.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP 5.3.22 or 5.4.12 or later, http://www.php.net/downloads.php

Affected Software/OS
PHP version before 5.3.22 and 5.4.x before 5.4.12

Vulnerability Insight
Flaws are due to the way SOAP parser process certain SOAP objects (due to allowed expansion of XML external entities during SOAP WSDL files parsing).

Vulnerability Detection Method
Get the installed version of PHP with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP SOAP Parser Multiple Information Disclosure Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.803764
Version used: `$Revision: 5351 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2013-1824`
`BID:62373`
`Other:`
`URL:http://php.net/ChangeLog-5.php`
`URL:http://git.php.net/?p=php-src.git;a=commit;h=afe98b7829d50806559acac9b530`
`↪acb8283c3bf4`

Medium (CVSS: 5.0)
NVT: PHP Version < 5.1.0 Multiple Vulnerabilities

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
PHP version smaller than 5.1.0 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.1.0

Solution
Solution type: VendorFix
Update PHP to version 5.1.0 or later.

Vulnerability Detection Method
Details:PHP Version < 5.1.0 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110170
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2005-3319, CVE-2005-3883
BID:15177, 15571

Medium (CVSS: 6.8)
NVT: PHP Version < 5.2.3 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
PHP version smaller than 5.2.3 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4

... continues on next page ...

... continued from previous page ...

Fixed version: 5.2.3

Solution
Solution type: VendorFix
Update PHP to version 5.2.3 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.3 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110189
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2007-1900, CVE-2007-2756, CVE-2007-2872, CVE-2007-3007
BID:23359, 24089, 24259, 24261

Medium (CVSS: 5.0)
NVT: PHP Version < 5.2.9 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.2.9 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.9

Solution
Solution type: VendorFix
Update PHP to version 5.2.9 or later.

Vulnerability Detection Method
Details:PHP Version < 5.2.9 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110187
Version used: $Revision: 4506 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-5498, CVE-2009-1271, CVE-2009-1272
BID:33002, 33927

Medium (CVSS: 6.8)
NVT: PHP Version < 5.3.4 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version smaller than 5.3.4 suffers from multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.4

Solution
Solution type: VendorFix
Update PHP to version 5.3.4 or later.

Vulnerability Detection Method
Details:PHP Version < 5.3.4 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110181
Version used: $Revision: 4506 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2006-7243, CVE-2010-2094, CVE-2010-2950, CVE-2010-3436, CVE-2010-3709,
↪CVE-2010-3710, CVE-2010-3870, CVE-2010-4150, CVE-2010-4156, CVE-2010-4409, CVE
↪-2010-4697, CVE-2010-4698, CVE-2010-4699, CVE-2010-4700, CVE-2011-0753, CVE-20
↪11-0754, CVE-2011-0755
BID:40173, 43926, 44605, 44718, 44723, 44951, 44980, 45119, 45335, 45338, 45339,

... continues on next page ...

... continued from previous page ...

↪ 45952, 45954, 46056, 46168

Medium (CVSS: 6.4)
NVT: PHP Version < 5.3.9 Multiple Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
PHP version < 5.3.9 suffers from multiple vulnerabilities such as DOS by sending crafted requests including hash collision parameter values. Several errors exist in some certain functions as well.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.3.9

Solution
Solution type: VendorFix
Upgrade PHP to 5.3.9 or versions after.

Vulnerability Detection Method
Details:PHP Version < 5.3.9 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.110012
Version used: $Revision: 4589 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2011-4566, CVE-2011-4885, CVE-2012-0057, CVE-2012-0781, CVE-2012-0788,
↪CVE-2012-0789
BID:50907, 51193, 51806, 51952, 51992, 52043

Medium (CVSS: 6.8)
NVT: PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103

... continues on next page ...

... continued from previous page ...

↪592)

Summary
This host is installed with PHP and is prone to XML entity expansion and XML external entity vulnerbilities

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 5.5.22`

Impact
Successfully exploiting this issue allow remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to PHP version 5.5.22, or 5.6.6, or later. For updates refer to http://www.php.net

Affected Software/OS
PHP versions prior to 5.5.22 and 5.6.x before 5.6.6 on Linux

Vulnerability Insight
The flaw is due to script 'ext/libxml/libxml.c' does not isolate each thread from 'libxml_disable_entity_loader' when PHP-FPM is used.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.808615
Version used: `$Revision: 5083 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2015-8866`
`BID:87470`
`Other:`
`URL:http://www.php.net/ChangeLog-5.php`

Medium (CVSS: 6.8)
NVT: PHP Zend and GD Multiple Denial of Service Vulnerabilities

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103592)

Summary
This host is running PHP and is prone to multiple denial of service vulnerabilities.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.15/5.3.5

Impact
Successful exploitation could allow local attackers to crash the affected application, denying service to legitimate users.
Impact Level: Application/Network

Solution
Solution type: VendorFix
Upgrade to PHP 5.3.5 or later For updates refer to http://www.php.net/downloads.php

Affected Software/OS
PHP version prior to 5.2.15 and 5.3.x before 5.3.4

Vulnerability Insight
The flaws are due to: - An use-after-free error in the 'Zend' engine, which allows remote attackers to cause a denial of service. - A stack-based buffer overflow in the 'GD' extension, which allows attackers to cause a denial of service.

Vulnerability Detection Method
Details:PHP Zend and GD Multiple Denial of Service Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.801586
Version used: $Revision: 4502 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2010-4697, CVE-2010-4698
Other:
URL:http://bugs.php.net/52879

... continues on next page ...

... continued from previous page ...

URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 5.0)
NVT: phpBB Account Re-Activation Authentication Bypass Vulnerability

Summary
According to its version number, the remote version of phpbb is prone to an authentication-bypass vulnerability because it fails to properly enforce privilege requirements on some operations.
Attackers can exploit this vulnerability to gain unauthorized access to the affected application, which may aid in further attacks.
Versions prior to phpBB 3.0.4 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available please see http://www.phpbb.com/.

Vulnerability Detection Method
Details:phpBB Account Re-Activation Authentication Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100086
Version used: $Revision: 5016 $

References
CVE: CVE-2008-6506
BID:32842
Other:
URL:http://www.securityfocus.com/bid/32842
URL:http://www.phpbb.com/

Medium (CVSS: 5.0)
NVT: phpBB Account Re-Activation Authentication Bypass Vulnerability

Summary
According to its version number, the remote version of phpbb is prone to an authentication-bypass vulnerability because it fails to properly enforce privilege requirements on some operations.
Attackers can exploit this vulnerability to gain unauthorized access to the affected application, which may aid in further attacks.
Versions prior to phpBB 3.0.4 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available please see http://www.phpbb.com/.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:phpBB Account Re-Activation Authentication Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100086
Version used: $Revision: 5016 $

References
CVE: CVE-2008-6506
BID:32842
Other:
URL:http://www.securityfocus.com/bid/32842
URL:http://www.phpbb.com/

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight
The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: $Revision: 5323 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2010-4480
Other:
URL:http://www.exploit-db.com/exploits/15699/
URL:http://www.vupen.com/english/advisories/2010/3133

Medium (CVSS: 5.0)
NVT: phpMyAdmin 'unserialize()' Remote Code Execution Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to a vulnerability that lets attackers execute arbitrary code in the context of the webserver process. This may facilitate unauthorized access or privilege escalation other attacks are also possible.
Versions prior to phpMyAdmin 3.0.0 or 2.11.10 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:phpMyAdmin 'unserialize()' Remote Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100589
Version used: $Revision: 5323 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2009-4605
BID:37861
Other:
URL:http://www.securityfocus.com/bid/37861
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-3.php

Medium (CVSS: 6.5)
NVT: phpMyAdmin Bookmark Security Bypass Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to a security-bypass vulnerability that affects bookmarks.
Successfully exploiting this issue allows a remote attacker to bypass certain security restrictions and perform unauthorized actions.
Versions prior to phpMyAdmin 3.3.9.2 and 2.11.11.3 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:phpMyAdmin Bookmark Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103076
Version used: $Revision: 3911 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2011-0987
BID:46359
Other:
URL:https://www.securityfocus.com/bid/46359
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2011-2.php

Medium (CVSS: 4.3)
NVT: phpMyAdmin Cross-Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
The host is running phpMyAdmin, which is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Execution of arbitrary HTML and script code will allow attackers to steal cookie-based authentication credentials and to launch other attacks. Impact Level : Application

Solution
Update to version 2.11.9.2 http://www.phpmyadmin.net/home_page/downloads.php
*** NOTE : Ignore this warning, if above mentioned Update is applied already. *****

Affected Software/OS
phpMyAdmin versions prior to 2.11.9.2 on all platform

Vulnerability Insight
Error exists in the PMA_escapeJsString() function in js_escape.lib.php file, which fails to sufficiently sanitize user-supplied data.

Vulnerability Detection Method
Details:phpMyAdmin Cross-Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900134
Version used: $Revision: 4522 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
BID:31327
Other:
URL:http://www.phpmyadmin.net/home_page/downloads.php?relnotes=1
URL:http://secunia.com/advisories/31974/
URL:http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2008-8

Medium (CVSS: 6.5)
NVT: phpMyAdmin DB_ Create.PHP Multiple Input Validation Vulnerabilities

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to multiple input-validation vulnerabilities, including a cross-site scripting and a SQL-injection issue.
A successful exploit may allow an attacker to steal cookie-based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.
These issues affect versions prior to phpMyAdmin 2.11.2.1.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:phpMyAdmin DB_Create.PHP Multiple Input Validation Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100067
Version used: $Revision: 5016 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2007-5976, CVE-2007-5977
BID:26512
Other:
URL:http://www.securityfocus.com/bid/26512

Medium (CVSS: 4.3)
NVT: PHProxy XSS

Summary
The remote host is running PHProxy, a web HTTP proxy written in PHP. There is a bug in the remote version software which makes it vulnerable to HTML and JavaScript injection.

Vulnerability Detection Result
. . . continues on next page . . .

... continued from previous page ...

Vulnerable url: http://192.168.27.45/beef/hook/index.php?error=<script>foo</scri
↪pt>

Impact
An attacker may use this bug to preform web cache poisoning, xss attack, etc.

Solution
Solution type: VendorFix
Upgrade to the newest version of this software

Vulnerability Detection Method
Details:PHProxy XSS
OID:1.3.6.1.4.1.25623.1.0.16069
Version used: $Revision: 6053 $

References
CVE: CVE-2004-2604
BID:12115

Medium (CVSS: 4.3)
NVT: PsNews XSS

Summary
The remote server is running a version of PsNews (a content management system) which is older than 1.2.
This version is affected by multiple cross-site scripting flaws. An attacker may exploit these to steal the cookies from legitimate users of this website.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45/beef/hook/index.php?function=add_kom&no=<sc
↪ript>foo</script>

Solution
Solution type: VendorFix
Upgrade to a newer version.

Vulnerability Detection Method
Details:PsNews XSS
OID:1.3.6.1.4.1.25623.1.0.14685
Version used: $Revision: 6046 $

References
CVE: CVE-2004-1665
BID:11124

Medium (CVSS: 5.0)
NVT: sgdynamo_xss

Summary
The remote host is running the CGI 'sgdynamo.exe'.
There is a bug in some versions of this CGI which makes it vulnerable to a cross site scripting attack.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/sgdynamo.exe?HTNAME=<script>foo</scrip`
`↪t>`

Solution
None at this time

Vulnerability Detection Method
Details:`sgdynamo_xss`
OID:1.3.6.1.4.1.25623.1.0.11955
Version used: `$Revision: 6056 $`

References
`CVE: CVE-2002-0375`
`BID:4720`

Medium (CVSS: 4.3)
NVT: Siteframe Cross Site Scripting Bugs

Summary
Siteframe 2.2.4 has a cross site scripting bug. An attacker may use it to perform a cross site scripting attack on this host.
In addition to this, another flaw in this package may allow an attacker to obtain the physical path to the remote web root.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/search.php?searchfor="><script>window.`
`↪alert(document.cookie);</script>`

Solution
Solution type: VendorFix
Upgrade to a newer version.

Vulnerability Detection Method
Details:`Siteframe Cross Site Scripting Bugs`
OID:1.3.6.1.4.1.25623.1.0.11448
Version used: `$Revision: 6046 $`

References

. . . continues on next page . . .

... continued from previous page ...

BID:7140, 7143

Medium (CVSS: 4.3)
NVT: SkaDate 'blogs.php' Cross Site Scripting Vulnerability

Summary
SkaDate is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45/info/blogs.php?tag=gamecat+<script>alert(/o
↪penvas-xss-test/)</script>

Impact
An attacker can exploit this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may help the attacker steal cookie-based authentication credentials and launch other attacks.

Vulnerability Detection Method
Details:SkaDate 'blogs.php' Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103269
Version used: $Revision: 3983 $

References
BID:49502
Other:
URL:http://www.securityfocus.com/bid/49502
URL:http://www.skadate.com

Medium (CVSS: 6.8)
NVT: SquirrelMail's Cross Site Scripting

Summary
The remote host seems to be vulnerable to a security problem in SquirrelMail. Its script 'read_body.php' didn't filter out user input for 'filter_dir' and 'mailbox', making a xss attack possible.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45/info/read_body.php?mailbox=<script>alert(do
↪cument.cookie)</script>&passed_id=<script>alert(document.cookie)</script>&star
↪tMessage=1&show_more=0

Solution
Solution type: VendorFix
Upgrade to a newer version of this software

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:SquirrelMail's Cross Site Scripting
OID:1.3.6.1.4.1.25623.1.0.11415
Version used: $Revision: 6046 $

References
CVE: CVE-2002-1276, CVE-2002-1341
BID:6302, 7019
Other:
RHSA:RHSA-2003:0042-07

Medium (CVSS: 5.0)
NVT: Turnkey eBook Store 'keywords' Parameter Cross Site Scripting Vulnerability

Summary
Turnkey eBook Store is prone to a cross-site scripting vulnerability.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site and to steal cookie-based authentication credentials.
Turnkey eBook Store 1.1 is vulnerable other versions may also be affected.

Vulnerability Detection Result
Vulnerable url: http://192.168.27.45/beef/hook/index.php?cmd=search&keywords="><
↪script>alert(document.cookie);</script>

Solution
Solution type: VendorFix

Vulnerability Detection Method
Details:Turnkey eBook Store 'keywords' Parameter Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100098
Version used: $Revision: 5768 $

References
BID:34324

Medium (CVSS: 4.3)
NVT: WordPress 'Non-Strict Mode' Multiple Cross-Site Scripting Vulnerabilities (Linux)

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

... continues on next page ...

... continued from previous page ...

Summary
This host is running WordPress and is prone to multiple cross site scripting vulnerabilities.

Vulnerability Detection Result
`Installed Version: 1.5.1.1`
`Fixed Version: 4.1.2`

Impact
Successful exploitation will allow remote attackers to execute arbitrary script code in a user's browser session within the trust relationship between their browser and the server.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 4.1.2 or higher, For updates refer https://wordpress.org

Affected Software/OS
Wordpress versions before 4.1.2 on Linux.

Vulnerability Insight
Multiple flaws exists due to improper input data sanitization via four-byte UTF-8 character or via an invalid character.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`WordPress 'Non-Strict Mode' Multiple Cross-Site Scripting Vulnerabilities (Linu.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.805988
Version used: `$Revision: 5087 $`

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:1.5.1.1`
Method: `WordPress Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
`CVE: CVE-2015-3438`
`BID:74269`
`Other:`
`URL:https://wordpress.org/news/2015/04/wordpress-4-1-2`
`URL:http://zoczus.blogspot.in/2015/04/plupload-same-origin-method-execution.h`
`↪tml`

Medium (CVSS: 6.8)
NVT: WordPress 'wp-admin/includes/file.php' Arbitrary File Upload Vulnerability

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
WordPress is prone to a vulnerability that lets attackers upload arbitrary files. The issue occurs because the application fails to adequately sanitize user-supplied input.
An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation other attacks are also possible.
Note that this issue only arises in certain Apache configurations that are using the Add* directives and PHP to facilitate handling of files with multiple extensions.
WordPress 2.8.5 and prior versions are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:WordPress 'wp-admin/includes/file.php' Arbitrary File Upload Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100345
Version used: $Revision: 5231 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
BID:37005
Other:
URL:http://www.securityfocus.com/bid/37005
URL:http://wordpress.org/
URL:http://www.securityfocus.com/archive/1/507819
URL:http://wordpress.org/development/2009/11/wordpress-2-8-6-security-release
↪/

Medium (CVSS: 6.8)
NVT: WordPress < 4.7.1 Multiple Security Vulnerabilities (Linux)

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

... continues on next page ...

... continued from previous page ...

Summary
This host is running WordPress and is prone to multiple security vulnerabilities.

Vulnerability Detection Result
`Installed version: 1.5.1.1`
`Fixed version: 4.7.1`

Impact
Successfully exploiting this issue allow remote attacker to e.g. obtain sensitive information or inject arbitrary web script or HTML.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to WordPress version 4.7.1. For updates refer to https://wordpress.org

Affected Software/OS
WordPress versions 4.7 and earlier on Linux.

Vulnerability Insight
Multiple flaws are due to:
- Cross-site scripting (XSS) via the plugin name or version header on update-core.php
- Cross-site request forgery (CSRF) bypass via uploading a Flash file
- Cross-site scripting (XSS) via theme name fallback
- Post via email checks mail.example.com if default settings are not changed
- Cross-site request forgery (CSRF) in the accessibility mode of widget editing
- Weak cryptographic security for multisite activation key

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check if the version is vulnerable or not.
Details:`WordPress < 4.7.1 Multiple Security Vulnerabilities (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108046
Version used: `$Revision: 5175 $`

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:1.5.1.1`
Method: `WordPress Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
`CVE: CVE-2017-5493, CVE-2017-5492, CVE-2017-5491, CVE-2017-5490, CVE-2017-5489,`
`↪CVE-2017-5488, CVE-2017-5487, CVE-2016-10066`
`Other:`

... continues on next page ...

... continued from previous page ...

URL:https://wpvulndb.com/wordpresses/47
URL:https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/

Medium (CVSS: 4.0)
NVT: WordPress _REQUEST array Cross Site Request Forgery (CSRF) Vulnerability

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
The host is installed with WordPress and is prone to Cross Site Request Forgery(CSRF) Vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful attack could lead to execution of arbitrary script code and can cause denial of service condition. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to WordPress version 2.9.2 or later For updates refer to http://wordpress.org/
NOTE: This issue relies on the presence of an independent vulnerability that allows cookie injection.

Affected Software/OS
WordPress 2.6.3 and earlier on all running platforms.

Vulnerability Insight
The flaw is due to incorrect usage of _REQUEST super global array, which leads to cross site request forgery (CSRF) attacks via crafted cookies.

Vulnerability Detection Method
Details:WordPress _REQUEST array Cross Site Request Forgery (CSRF) Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800140
Version used: $Revision: 4227 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2008-5113
Other:
URL:http://openwall.com/lists/oss-security/2008/11/14/1
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=504771

Medium (CVSS: 4.3)
NVT: WordPress Comment Author URI Cross-Site Scripting Vulnerability

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
WordPress is prone to a cross-site scripting vulnerability because the application fails to properly sanitize user-supplied input.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may help the attacker steal cookie-based authentication credentials and launch other attacks.
Versions prior to WordPress 2.8.2 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
The vendor has released an update. Please see the references for details.

Vulnerability Detection Method
Details:WordPress Comment Author URI Cross-Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100239
Version used: $Revision: 5231 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
CVE: CVE-2009-2851
BID:35755
Other:
URL:http://www.securityfocus.com/bid/35755
URL:http://bugs.gentoo.org/show_bug.cgi?id=278492
URL:http://wordpress.org/development/2009/07/wordpress-2-8-2/

... continues on next page ...

... continued from previous page ...

URL:http://wordpress.org/

Medium (CVSS: 6.8)
NVT: WordPress Core Multiple Vulnerabilities May16 (Linux)

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
This host is running WordPress and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.5.1.1
Fixed version: 4.5

Impact
Successfully exploiting this issue allows remote attacker to conduct XSS, CSRF and SSRF bypass attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to WordPress version 4.5 or later. For updates refer to https://wordpress.org

Affected Software/OS
WordPress versions prior to 4.5 on Linux.

Vulnerability Insight
Multiple flaws are due to, - An improper validation of HTTP request for detection of valid IP addresses. - An insufficient validation in network setting. - A script compression option CSRF.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:WordPress Core Multiple Vulnerabilities May16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808035
Version used: $Revision: 5836 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2016-4029, CVE-2016-6634, CVE-2016-6635
BID:92400, 92390, 92355
Other:
URL:https://wpvulndb.com/vulnerabilities/8473
URL:https://wpvulndb.com/vulnerabilities/8474
URL:https://wpvulndb.com/vulnerabilities/8475
URL:https://codex.wordpress.org/Version_4.5#Security

Medium (CVSS: 4.3)
NVT: WordPress MU Cross-Site Scripting Vulnerability - Apr09

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
The host is running WordPress MU and is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let the attacker execute malicious crafted HTTP headers and conduct cross site scripting attacks to gain administrative privileges into the affected web application.
Impact Level: Application

Solution
Update to Version 2.7 http://mu.wordpress.org/download

Affected Software/OS
WordPress MU before 2.7 on all running platform.

Vulnerability Insight
The vulnerability is due to improper validation of user supplied input in 'wp-includes/wpmu-functions.php' for choose_primary_blog function.

Vulnerability Detection Method
Details:WordPress MU Cross-Site Scripting Vulnerability - Apr09
OID:1.3.6.1.4.1.25623.1.0.800376
Version used: $Revision: 4970 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2009-1030
BID:34075
Other:
URL:http://www.milw0rm.com/exploits/8196
URL:http://xforce.iss.net/xforce/xfdb/49184
URL:http://securitytracker.com/alerts/2009/Mar/1021838.html

Medium (CVSS: 5.0)
NVT: WordPress MU Multiple Vulnerabilities - July09

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
The host is running WordPress MU and is prone to Multiple Vulnerabilities

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to view the content of plugins configuration pages, inject malicious scripting code, or gain knowledge of sensitive username information. Impact Level: Application

Solution
Update to Version 2.8.1 http://mu.wordpress.org/download/

Affected Software/OS
WordPress MU version prior to 2.8.1 on all running platform.

Vulnerability Insight
- Error in 'wp-settings.php' which may disclose the sensitive information via a direct request. - Error occur when user attampt for failed login or password request depending on whether the user account exists, and it can be exploited by enumerate valid usernames. - Error in wp-admin/admin.php is does not require administrative authentication to access the configuration of a plugin, which allows attackers to specify a configuration file in the page parameter via collapsing-archives/options.txt, related-ways-to-take-action/options.php, wp-security-scan/securityscan.php, akismet/readme.txt and wp-ids/ids-admin.php.

Vulnerability Detection Method
Details:WordPress MU Multiple Vulnerabilities - July09
OID:1.3.6.1.4.1.25623.1.0.800662

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 4970 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
CVE: CVE-2009-2432, CVE-2009-2336, CVE-2009-2335, CVE-2009-2334
BID:35581, 35584
Other:
URL:http://www.vupen.com/english/advisories/2009/1833
URL:http://securitytracker.com/alerts/2009/Jul/1022528.html
URL:http://www.securityfocus.com/archive/1/archive/1/504795/100/0/threaded

Medium (CVSS: 5.0)
NVT: WordPress Multiple Vulnerabilities - July09

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
The host is running WordPress and is prone to Multiple Vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to view the content of plugins configuration pages, inject malicious scripting code, or gain knowledge of sensitive username information. Impact Level: Application

Solution
Update to Version 2.8.1 http://wordpress.org/download/

Affected Software/OS
WordPress version prior to 2.8.1 on all running platform.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

- Error in 'wp-settings.php' which may disclose the sensitive information via a direct request. - username of a post's author is placed in an HTML comment, which allows remote attackers to obtain sensitive information by reading the HTML source. - Error occur when user attampt for failed login or password request depending on whether the user account exists, and it can be exploited by enumerate valid usernames. - wp-admin/admin.php does not require administrative authentication to access the configuration of a plugin, which allows attackers to specify a configuration file in the page parameter via collapsing-archives/options.txt, related-ways-to-take-action/options.php, wp-security-scan/securityscan.php, akismet/readme.txt and wp-ids/ids-admin.php.

Vulnerability Detection Method
Details:`WordPress Multiple Vulnerabilities - July09`
OID:1.3.6.1.4.1.25623.1.0.800657
Version used: `$Revision: 4970 $`

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:1.5.1.1`
Method: `WordPress Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
```
CVE: CVE-2009-2432, CVE-2009-2431, CVE-2009-2336, CVE-2009-2335, CVE-2009-2334
BID:35581, 35584
Other:
  URL:http://www.vupen.com/english/advisories/2009/1833
   URL:http://securitytracker.com/alerts/2009/Jul/1022528.html
   URL:http://www.securityfocus.com/archive/1/archive/1/504795/100/0/threaded
```

Medium (CVSS: 6.0)
NVT: WordPress Multiple Vulnerabilities - Nov09

Product detection result
```
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)
```

Summary
The host is running WordPress and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Attackers can exploit this issue to execute arbitrary PHP code by uploading malicious PHP files and to inject arbitrary web script or HTML code which will be executed in a user's browser session Impact Level: System/Application

Solution
Update to Version 2.8.6 http://wordpress.org/download/

Affected Software/OS
WordPress version prior to 2.8.6 on all running platform.

Vulnerability Insight
- The 'wp_check_filetype()' function in /wp-includes/functions.php does not properly validate files before uploading them. - Input passed into the 's' parameter in press-this.php is not sanitised before being displayed to the user.

Vulnerability Detection Method
Details:`WordPress Multiple Vulnerabilities - Nov09`
OID:1.3.6.1.4.1.25623.1.0.900975
Version used: `$Revision: 5148 $`

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:1.5.1.1`
Method: `WordPress Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
```
CVE: CVE-2009-3890, CVE-2009-3891
BID:37014, 37005
Other:
  URL:http://secunia.com/advisories/37332
   URL:http://www.openwall.com/lists/oss-security/2009/11/15/2
```

Medium (CVSS: 5.0)
NVT: WordPress Multiple Vulnerabilities July16 (Linux)

Product detection result
```
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)
```

Summary
This host is running WordPress and is prone to multiple vulnerabilities.

Vulnerability Detection Result
`Installed version: 1.5.1.1`

... continues on next page ...

... continued from previous page ...

Fixed version: 4.5.3

Impact
Successfully exploiting this issue allow remote attacker to inject arbitrary web script or HTML, obtain sensitive information, bypass intended redirection restrictions, cause a denial of service and bypass intended password-change restrictions.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to WordPress version 4.5.3 or later. For updates refer to https://wordpress.org

Affected Software/OS
WordPress versions prior to 4.5.3 on Linux.

Vulnerability Insight
Multiple flaws are due to, - An insufficient validation of user supplied input via attachment name in the column_title function in 'wp-admin/includes/class-wp-media-list-table.php' script. - An error related to 'wp-admin/includes/ajax-actions.php' and 'wp-admin/revision.php' scripts. - An error in customizer. - An insufficient validation of user supplied input via attachment name in the wp_get_attachment_link function in 'wp-includes/post-template.php' script. - An error in 'oEmbed' protocol implementation. - Other multiple unspecified errors.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:WordPress Multiple Vulnerabilities July16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808256
Version used: $Revision: 5588 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
CVE: CVE-2016-5832, CVE-2016-5833, CVE-2016-5834, CVE-2016-5835, CVE-2016-5836,
↪CVE-2016-5837, CVE-2016-5838, CVE-2016-5839
BID:91362, 91368, 91366, 91363, 91365, 91367, 91364
Other:
URL:https://wordpress.org/news/2016/06/wordpress-4-5-3

Medium (CVSS: 5.8)
NVT: WordPress Multiple Vulnerabilities Mar17 (Linux)

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1

... continues on next page ...

... continued from previous page ...

Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
This host is running WordPress and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 1.5.1.1
Fixed version: 4.7.3

Impact
Successfully exploiting will allow remote attacker to create a specially crafted URL,execute arbitrary script code in a user's browser session within the trust relationship between their browser and the server and leading to excessive use of server resources.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to WordPress 4.7.3 or later, For updates refer to https://wordpress.org

Affected Software/OS
WordPress versions 4.7.2 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to, - A cross-site scripting (XSS) vulnerability in media file metadata. - An improper URL validation. - Unintended files can be deleted by administrators using the plugin deletion functionality. - A cross-site scripting (XSS) in video URL in YouTube embeds. - A Cross-site request forgery (CSRF) in Press.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:WordPress Multiple Vulnerabilities Mar17 (Linux)
OID:1.3.6.1.4.1.25623.1.0.809896
Version used: $Revision: 5606 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
CVE: CVE-2017-6804, CVE-2017-6815, CVE-2017-6814, CVE-2017-6816, CVE-2017-6818,
↪CVE-2017-6817, CVE-2017-6819
Other:
URL:https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenanc
↪e-release

Medium (CVSS: 5.0)
NVT: WordPress Password Protection Security Bypass Vulnerability

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
WordPress is prone to a security-bypass vulnerability.
Attackers may exploit this issue to access certain content that may contain sensitive information.
WordPress 2.9.2 and 2.0.11 are vulnerable other versions may also be affected.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Vulnerability Detection Method
Details:WordPress Password Protection Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100549
Version used: $Revision: 5388 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
BID:38876
Other:
URL:http://www.securityfocus.com/bid/38876
URL:http://seclists.org/fulldisclosure/2010/Mar/361
URL:http://wordpress.org/

Medium (CVSS: 4.3)
NVT: WordPress Same Origin Method Execution Vulnerability May16 (Linux)

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
This host is running WordPress and is prone to same origin method execution vulnerability.

Vulnerability Detection Result
Installed version: 1.5.1.1

... continues on next page ...

... continued from previous page ...

Fixed version: 4.5.2

Impact
Successfully exploiting this issue allow remote attacker to execute arbitrary script code on the endpoint's domain.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to WordPress version 4.5.2 or later, For updates refer to https://wordpress.org

Affected Software/OS
WordPress versions prior to 4.5.2 on Linux.

Vulnerability Insight
The flaw exist due to an error in wordpress Plupload library used for uploading files.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:WordPress Same Origin Method Execution Vulnerability May16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808049
Version used: $Revision: 5534 $

Product Detection Result
Product: cpe:/a:wordpress:wordpress:1.5.1.1
Method: WordPress Version Detection
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
Other:
URL:https://wordpress.org/news/2016/05/wordpress-4-5-2

Medium (CVSS: 4.0)
NVT: WordPress Trashed Posts Information Disclosure Vulnerability

Product detection result
cpe:/a:wordpress:wordpress:1.5.1.1
Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary
WordPress is prone to an information-disclosure vulnerability because it fails to properly restrict access to trashed posts.
An attacker can exploit this vulnerability to view other authors' trashed posts, which may aid in further attacks.

... continues on next page ...

... continued from previous page ...

Versions prior to WordPress 2.9.2 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:`WordPress Trashed Posts Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100505
Version used: `$Revision: 5401 $`

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:1.5.1.1`
Method: `WordPress Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
```
CVE: CVE-2010-0682
BID:38368
Other:
  URL:http://www.securityfocus.com/bid/38368
   URL:http://tmacuk.co.uk/?p=180
   URL:http://wordpress.org/development/2010/02/wordpress-2-9-2/
   URL:http://wordpress.org/
```

Medium (CVSS: 4.3)
NVT: WordPress wp-trackback.php Denial of Service Vulnerability

Product detection result
`cpe:/a:wordpress:wordpress:1.5.1.1`
`Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)`

Summary
The host is running WordPress and is prone to Denial of Service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attacker to cause a Denial of Service due to high CPU consumption. Impact Level: System/Application

... continues on next page ...

... continued from previous page ...

Solution
Upgrade to WordPress version 2.8.5 or later. http://wordpress.org/download/

Affected Software/OS
WordPress version prior to 2.8.5 on all platforms.

Vulnerability Insight
An error occurs in wp-trackbacks.php due to improper validation of user supplied data passed into 'mb_convert_encoding()' function. This can be exploited by sending multiple-source character encodings into the fuction.

Vulnerability Detection Method
Details:`WordPress wp-trackback.php Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.900968
Version used: `$Revision: 5148 $`

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:1.5.1.1`
Method: `WordPress Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
```
CVE: CVE-2009-3622
Other:
  URL:http://secunia.com/advisories/37088/
   URL:http://www.milw0rm.com/exploits/9431
   URL:http://xforce.iss.net/xforce/xfdb/53884
   URL:http://www.vupen.com/english/advisories/2009/2986
```

[return to 192.168.27.45]

2.1.8 Medium 5432/tcp

Medium (CVSS: 4.0)
NVT: PostgreSQL Denial of Service Vulnerability (Linux)

Summary
This host is installed with PostgreSQL Server and is prone to denial of service vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let the attacker cause stack consumption or denial of service through mismatched encoding conversion requests.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to respective version below, PostgreSQL 8.3.7 or 8.2.13 or 8.1.17 or 8.0.21 or 7.4.25 http://www.postgresql.org

Affected Software/OS
PostgreSQL versions before 8.3.7, 8.2.13, 8.1.17, 8.0.21, and 7.4.25

Vulnerability Insight
This flaw is due to failure in converting a localized error message to the client-specified encoding.

Vulnerability Detection Method
Details:`PostgreSQL Denial of Service Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900480
Version used: `$Revision: 5122 $`

References
`CVE: CVE-2009-0922`
`BID:34090`
`Other:`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=488156`
`URL:http://archives.postgresql.org/pgsql-bugs/2009-02/msg00172.php`

[return to 192.168.27.45]

2.1.9 Low general/tcp

Low (CVSS: 2.1)
NVT: Firefox Information Disclosure Vulnerability Jan09 (Linux)

Summary
The host is installed with Mozilla Firefox browser and is prone to information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let the attacker execute arbitrary codes in the context of the web browser and can obtain sensitive information of the remote user through the web browser. Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Mozilla Firefox version 3.6.3 or later For updates refer to http://www.getfirefox.com

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Mozilla Firefox version from 2.0 to 3.0.5 on Linux.

Vulnerability Insight
The Web Browser fails to properly enforce the same-origin policy, which leads to cross-domain information disclosure.

Vulnerability Detection Method
Details:`Firefox Information Disclosure Vulnerability Jan09 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900449
Version used: `$Revision: 5055 $`

References
`CVE: CVE-2009-5913`
`BID:33276`
`Other:`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=480938`
`URL:http://www.trusteer.com/files/In-session-phishing-advisory-2.pdf`

Low (CVSS: 2.1)
NVT: PHP 'mbstring.func_overload' DoS Vulnerability

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
The host is running PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 4.4.5/5.1.7/5.2.6`

Impact
Successful exploitation will let the local attackers to crash an affected web server. Impact Level: Application

Solution
Solution type: VendorFix
Apply patch from below link, http://php.net

Affected Software/OS
PHP version 4.4.4 and prior PHP 5.1.x to 5.1.6 PHP 5.2.x to 5.2.5

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
This bug is due to an error in 'mbstring.func_overload' setting in .htaccess file. It can be exploited via modifying behavior of other sites hosted on the same web server which causes this setting to be applied to other virtual hosts on the same server.

Vulnerability Detection Method
Details:PHP 'mbstring.func_overload' DoS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800373
Version used: $Revision: 4504 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2009-0754
BID:33542
Other:
URL:http://bugs.php.net/bug.php?id=27421
URL:https://bugzilla.redhat.com/show_bug.cgi?id=479272

Low (CVSS: 2.6)
NVT: PHP display_errors Cross-Site Scripting Vulnerability

Product detection result
cpe:/a:php:php:4.4.4
Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103
↪592)

Summary
The host is running PHP and is prone to Cross-Site Scripting vulnerability.

Vulnerability Detection Result
Installed version: 4.4.4
Fixed version: 5.2.8

Impact
Successful exploitation could allow attackers to inject arbitrary web script or HTML via unspecified vectors and conduct Cross-Site Scripting attacks.
Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to version 5.2.8 or later http://www.php.net/downloads.php

Affected Software/OS
PHP version 5.2.7 and prior on all running platform.

Vulnerability Insight
The flaw is due to improper handling of certain inputs when display_errors settings is enabled.

Vulnerability Detection Method
Details:PHP display_errors Cross-Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800334
Version used: $Revision: 4504 $

Product Detection Result
Product: cpe:/a:php:php:4.4.4
Method: PHP Version Detection (Linux, local)
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
CVE: CVE-2008-5814
Other:
URL:http://jvn.jp/en/jp/JVN50327700/index.html
URL:http://jvndb.jvn.jp/en/contents/2008/JVNDB-2008-000084.html

Low (CVSS: 2.1)
NVT: ProFTPD 'AllowChrootSymlinks' Local Security Bypass Vulnerability

Product detection result
cpe:/a:proftpd:proftpd:1.3.0
Detected by ProFTPD Server Version Detection (Local) (OID: 1.3.6.1.4.1.25623.1.0
↪.900506)

Summary
This host is running ProFTPD server and is prone to local security bypass vulnerability.

Vulnerability Detection Result
Installed version: 1.3.0
Fixed version: 1.3.5e/1.3.6rc5

Impact
Successful exploitation will allows attackers to bypass certain security restrictions and perform unauthorized actions.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade ProFTPD 1.3.5e, 1.3.6rc5 or later, For updates refer to http://www.proftpd.org

Affected Software/OS
ProFTPD versions prior to 1.3.5e and 1.3.6 prior to 1.3.6rc5 are vulnerable.

Vulnerability Insight
The ProFTPD controls whether the home directory of a user could contain a symbolic link through the AllowChrootSymlinks configuration option, but checks only the last path component when enforcing AllowChrootSymlinks.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:`ProFTPD 'AllowChrootSymlinks' Local Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.810731
Version used: `$Revision: 5962 $`

Product Detection Result
Product: `cpe:/a:proftpd:proftpd:1.3.0`
Method: `ProFTPD Server Version Detection (Local)`
OID: 1.3.6.1.4.1.25623.1.0.900506)

References
`CVE: CVE-2017-7418`
`BID:97409`
`Other:`
`URL:http://bugs.proftpd.org/show_bug.cgi?id=4295`
`URL:https://github.com/proftpd/proftpd/commit/ecff21e0d0e84f35c299ef91d7fda08`
`↪8e516d4ed`
`URL:https://github.com/proftpd/proftpd/commit/f59593e6ff730b832dbe8754916cb5c`
`↪821db579f`
`URL:https://github.com/proftpd/proftpd/pull/444/commits/349addc3be4fcdad9bd4e`
`↪c01ad1ccd916c898ed8`

Low (CVSS: 2.6)
NVT: Slackware Advisory SSA:2006-307-02 screen

Summary
The remote host is missing an update as announced via advisory SSA:2006-307-02.

Vulnerability Detection Result
`Package screen-4.0.2-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-307-02

Vulnerability Insight
New screen packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-307-02 screen`
OID:1.3.6.1.4.1.25623.1.0.57700
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2006-4573`

Low (CVSS: 2.6)
NVT: Slackware Advisory SSA:2006-307-02 screen

Summary
The remote host is missing an update as announced via advisory SSA:2006-307-02.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-307-02

Vulnerability Insight
New screen packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-307-02 screen`
OID:1.3.6.1.4.1.25623.1.0.57700
Version used: `$Revision: 5940 $`

References
`CVE: CVE-2006-4573`

Low (CVSS: 2.6)
NVT: Slackware Advisory SSA:2006-335-03 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2006-335-03.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`Package libpng-1.2.12-i486-2 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-335-03

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-335-03 libpng`
OID:1.3.6.1.4.1.25623.1.0.57702
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2006-5793`

Low (CVSS: 2.6)
NVT: Slackware Advisory SSA:2006-335-03 libpng

Summary
The remote host is missing an update as announced via advisory SSA:2006-335-03.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2006-335-03

Vulnerability Insight
New libpng packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, and 11.0 to fix security issues.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2006-335-03 libpng`
OID:1.3.6.1.4.1.25623.1.0.57702
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2006-5793`

Low (CVSS: 2.6)
NVT: Slackware Advisory SSA:2009-336-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2009-336-01.

Vulnerability Detection Result
`Package bind-9.3.2_P1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-336-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix a security issue.
More details about this issue may be found here: http://www.kb.cert.org/vuls/id/418861

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-336-01 bind`
OID:1.3.6.1.4.1.25623.1.0.66461
Version used: `$Revision: 5988 $`

References
`CVE: CVE-2009-4022`

Low (CVSS: 2.6)
NVT: Slackware Advisory SSA:2009-336-01 bind

Summary
The remote host is missing an update as announced via advisory SSA:2009-336-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2009-336-01

Vulnerability Insight
New bind packages are available for Slackware 8.1, 9.0, 9.1, 10.0, 10.1, 10.2, 11.0, 12.0, 12.1, 12.2, 13.0, and -current to fix a security issue.
More details about this issue may be found here: http://www.kb.cert.org/vuls/id/418861

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2009-336-01 bind`
OID:1.3.6.1.4.1.25623.1.0.66461

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 5988 $`

References
`CVE: CVE-2009-4022`

Low (CVSS: 3.7)
NVT: Slackware Advisory SSA:2011-108-01 acl

Summary
The remote host is missing an update as announced via advisory SSA:2011-108-01.

Vulnerability Detection Result
`Package acl-2.2.39_1-i486-1 is installed which is known to be vulnerable.`

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-108-01

Vulnerability Insight
New acl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-108-01 acl`
OID:1.3.6.1.4.1.25623.1.0.69578
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2009-4411`

Low (CVSS: 3.7)
NVT: Slackware Advisory SSA:2011-108-01 acl

Summary
The remote host is missing an update as announced via advisory SSA:2011-108-01.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Solution type: VendorFix
https://secure1.securityspace.com/smysecure/catid.html?in=SSA:2011-108-01

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

New acl packages are available for Slackware 11.0, 12.0, 12.1, 12.2, 13.0, 13.1, and -current to fix a security issue.

Vulnerability Detection Method
Details:`Slackware Advisory SSA:2011-108-01 acl`
OID:1.3.6.1.4.1.25623.1.0.69578
Version used: `$Revision: 5999 $`

References
`CVE: CVE-2009-4411`

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1892570
Packet 2: 1892836
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details:`TCP timestamps`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.80091
Version used: $Revision: 5740 $

References
Other:
URL:http://www.ietf.org/rfc/rfc1323.txt

[return to 192.168.27.45]

2.1.10 Low 22/tcp

Low (CVSS: 2.1)
NVT: OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability

Summary
OpenSSH is prone to a local information-disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Local attackers can exploit this issue to obtain sensitive information. Information obtained may lead to further attacks.

Solution
Updates are available.

Affected Software/OS
Versions prior to OpenSSH 5.8p2 are vulnerable.

Vulnerability Insight
ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.

Vulnerability Detection Method
Check the version.
Details:OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105002
Version used: $Revision: 4336 $

References
CVE: CVE-2011-4327
BID:65674
Other:
URL:http://www.securityfocus.com/bid/65674

... continues on next page ...

... continued from previous page ...

URL:http://www.openssh.com
URL:http://www.openssh.com/txt/portable-keysign-rand-helper.adv

Low (CVSS: 3.5)
NVT: OpenSSH 'ssh_gssapi_parse_ename()' Function Denial of Service Vulnerability

Summary
OpenSSH is prone to a remote denial-of-service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Exploiting this issue allows remote attackers to trigger denial-of-service conditions due to excessive memory consumption.

Solution
Updates are available. Please see the references for details.

Affected Software/OS
OpenSSH 5.8 and prior are vulnerable.

Vulnerability Detection Method
Check the version.
Details:OpenSSH 'ssh_gssapi_parse_ename()' Function Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103937
Version used: $Revision: 4336 $

References
CVE: CVE-2011-5000
BID:54114
Other:
URL:http://www.securityfocus.com/bid/54114
URL:http://www.openssh.com

Low (CVSS: 2.6)
NVT: OpenSSH CBC Mode Information Disclosure Vulnerability

Summary
The host is installed with OpenSSH and is prone to information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact

... continues on next page ...

... continued from previous page ...

Successful exploits will allow attackers to obtain four bytes of plaintext from an encrypted session.
Impact Level: Application

Solution
Upgrade to higher version http://www.openssh.com/portable.html

Affected Software/OS
Versions prior to OpenSSH 5.2 are vulnerable. Various versions of SSH Tectia are also affected.

Vulnerability Insight
The flaw is due to the improper handling of errors within an SSH session encrypted with a block cipher algorithm in the Cipher-Block Chaining 'CBC' mode.

Vulnerability Detection Method
Details:`OpenSSH CBC Mode Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100153
Version used: `$Revision: 5002 $`

References
`CVE: CVE-2008-5161`
`BID:32319`
`Other:`
`URL:http://www.securityfocus.com/bid/32319`

Low (CVSS: 3.5)
NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability

Summary
The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.

Vulnerability Detection Result
```
According to its banner, the version of OpenSSH installed on the remote
host is older than 5.7:
 SSH-1.99-OpenSSH_4.4
```

Solution
Updates are available. Please see the references for more information.

Affected Software/OS
OpenSSH before 5.7

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:openssh-server Forced Command Handling Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103503
Version used: $Revision: 5950 $

References
CVE: CVE-2012-0814
BID:51702
Other:
URL:http://www.securityfocus.com/bid/51702
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445
URL:http://packages.debian.org/squeeze/openssh-server
URL:https://downloads.avaya.com/css/P8/documents/100161262

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary
The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96

Solution
Solution type: Mitigation
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details:SSH Weak MAC Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: $Revision: 4490 $

[return to 192.168.27.45]

2.1.11 Low 80/tcp

Low (CVSS: 2.6)
NVT: NewsPortal 'post.php' Cross Site Scripting Vulnerability

Summary
NewsPortal is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input before using it in dynamically generated content.

Vulnerability Detection Result
`Vulnerable url: http://192.168.27.45/info/post.php?newsgroups=<script>alert('ope`
`↪nvas-xss-test')</script>`

Impact
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks.

Affected Software/OS
NewsPortal 0.37 is vulnerable other versions may also be affected.

Vulnerability Detection Method
Details:`NewsPortal 'post.php' Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103130
Version used: `$Revision: 3793 $`

References
`BID:46961`
`Other:`
`URL:https://www.securityfocus.com/bid/46961`
`URL:http://florian-amrhein.de/newsportal`

Low (CVSS: 2.1)
NVT: PHP 'mbstring.func_overload' DoS Vulnerability

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
The host is running PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 4.4.4`
`Fixed version: 4.4.5/5.1.7/5.2.6`

Impact

. . . continues on next page . . .

... continued from previous page ...

Successful exploitation will let the local attackers to crash an affected web server. Impact Level: Application

Solution
Solution type: VendorFix
Apply patch from below link, http://php.net

Affected Software/OS
PHP version 4.4.4 and prior PHP 5.1.x to 5.1.6 PHP 5.2.x to 5.2.5

Vulnerability Insight
This bug is due to an error in 'mbstring.func_overload' setting in .htaccess file. It can be exploited via modifying behavior of other sites hosted on the same web server which causes this setting to be applied to other virtual hosts on the same server.

Vulnerability Detection Method
Details:`PHP 'mbstring.func_overload' DoS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800373
Version used: `$Revision: 4504 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2009-0754`
`BID:33542`
`Other:`
`URL:http://bugs.php.net/bug.php?id=27421`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=479272`

Low (CVSS: 2.6)
NVT: PHP display_errors Cross-Site Scripting Vulnerability

Product detection result
`cpe:/a:php:php:4.4.4`
`Detected by PHP Version Detection (Linux, local) (OID: 1.3.6.1.4.1.25623.1.0.103`
`↪592)`

Summary
The host is running PHP and is prone to Cross-Site Scripting vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 4.4.4
Fixed version:     5.2.8
```

Impact
Successful exploitation could allow attackers to inject arbitrary web script or HTML via unspecified vectors and conduct Cross-Site Scripting attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 5.2.8 or later http://www.php.net/downloads.php

Affected Software/OS
PHP version 5.2.7 and prior on all running platform.

Vulnerability Insight
The flaw is due to improper handling of certain inputs when display_errors settings is enabled.

Vulnerability Detection Method
Details:`PHP display_errors Cross-Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800334
Version used: `$Revision: 4504 $`

Product Detection Result
Product: `cpe:/a:php:php:4.4.4`
Method: `PHP Version Detection (Linux, local)`
OID: 1.3.6.1.4.1.25623.1.0.103592)

References
`CVE: CVE-2008-5814`
`Other:`
`URL:http://jvn.jp/en/jp/JVN50327700/index.html`
`URL:http://jvndb.jvn.jp/en/contents/2008/JVNDB-2008-000084.html`

Low (CVSS: 2.6)
NVT: phpBB 'includes/message_parser.php' HTML Injection Vulnerability

Summary
phpBB is prone to an HTML-injection vulnerability because it fails to properly sanitize user-supplied input.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials, control how the site is rendered to the user, or launch other attacks.
Versions prior to phpBB 3.0.8 are vulnerable.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
The vendor has released updates. Please contact the vendor for details.

Vulnerability Detection Method
Details:phpBB 'includes/message_parser.php' HTML Injection Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100922
Version used: $Revision: 5323 $

References
BID:45005
Other:
URL:https://www.securityfocus.com/bid/45005
URL:http://www.phpbb.com/
URL:http://www.phpbb.com/support/documents.php?mode=changelog&version=3#v307-PL1

Low (CVSS: 2.6)
NVT: phpBB 'includes/message_parser.php' HTML Injection Vulnerability

Summary
phpBB is prone to an HTML-injection vulnerability because it fails to properly sanitize user-supplied input.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials, control how the site is rendered to the user, or launch other attacks.
Versions prior to phpBB 3.0.8 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
The vendor has released updates. Please contact the vendor for details.

Vulnerability Detection Method
Details:phpBB 'includes/message_parser.php' HTML Injection Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100922
Version used: $Revision: 5323 $

References
BID:45005
Other:
URL:https://www.securityfocus.com/bid/45005
URL:http://www.phpbb.com/

... continues on next page ...

... continued from previous page ...

URL:http://www.phpbb.com/support/documents.php?mode=changelog&version=3#v307-
↪PL1

Low (CVSS: 2.6)
NVT: phpMyAdmin pmd_pdf.php Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
This host is running phpMyAdmin and is prone to cross site scripting vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Allows execution of arbitrary HTML and script code, and steal cookie-based authentication credentials. Impact Level: System

Solution
Upgrade to phpMyAdmin 3.0.1.1 or later

Affected Software/OS
phpMyAdmin phpMyAdmin versions 3.0.1 and prior on all running platform.

Vulnerability Insight
Input passed to the 'db' parameter in pmd_pdf.php file is not properly sanitised before returning to the user.

Vulnerability Detection Method
Details:phpMyAdmin pmd_pdf.php Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800301
Version used: $Revision: 4227 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2008-4775
BID:31928
Other:

... continues on next page ...

... continued from previous page ...

URL:http://secunia.com/advisories/32449/
URL:http://seclists.org/bugtraq/2008/Oct/0199.html

[return to 192.168.27.45]

2.1.12 Log general/tcp

Log (CVSS: 0.0)
NVT: Adobe Flash Player/AIR Version Detection (Linux)

Summary
Detection of installed version of Adobe Flash Player/AIR on Windows.
The script logs in via ssh, extracts the version from the binary file and set it in KB.

Vulnerability Detection Result
```
Detected Adobe Flash Player
Version:  7.0.63.0
Location: /usr/lib/mozilla/plugins/libflashplayer.so
CPE:      cpe:/a:adobe:flash_player:7.0.63.0
Concluded from version/product identification result:
7.0.63.0
```

Log Method
Details:Adobe Flash Player/AIR Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800032
Version used: $Revision: 6032 $

Log (CVSS: 0.0)
NVT: Adobe Flash Player/AIR Version Detection (Linux)

Summary
Detection of installed version of Adobe Flash Player/AIR on Windows.
The script logs in via ssh, extracts the version from the binary file and set it in KB.

Vulnerability Detection Result
```
Detected Adobe Flash Player
Version:  9.0.31.0
Location: /opt/firefox/plugins/libflashplayer.so
CPE:      cpe:/a:adobe:flash_player:9.0.31.0
Concluded from version/product identification result:
9.0.31.0
```

Log Method
Details:Adobe Flash Player/AIR Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800032

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 6032 $

Log (CVSS: 0.0)
NVT: Adobe products version detection (Linux)

Summary
Detection of installed version of Adobe Products.
This script retrieves all Adobe Products version and saves those in KB.

Vulnerability Detection Result
```
Detected Adobe Reader
Version:  7.0.5
Location: /usr/lib/Adobe/Acrobat7.0/Reader/AcroVersion
CPE:      cpe:/a:adobe:acrobat_reader:7.0.5
Concluded from version/product identification result:
7.0.5
```

Log Method
Details:Adobe products version detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800108
Version used: $Revision: 6040 $

Log (CVSS: 0.0)
NVT: CTorrent/Enhanced CTorrent Version Detection

Summary
This script retrieves CTorrent/Enhanced CTorrent version and saves the result in KB.

Vulnerability Detection Result
```
Detected CTorrent/Enhanced CTorrent
Version:  2
Location: /usr/bin/ctorrent
stderr
CPE:      cpe:/a:rahul:dtorrent:2
Concluded from version/product identification result:
2
```

Log Method
Details:CTorrent/Enhanced CTorrent Version Detection
OID:1.3.6.1.4.1.25623.1.0.900556
Version used: $Revision: 5943 $

... continues on next page ...

... continued from previous page ...

Log (CVSS: 0.0)
NVT: CTorrent/Enhanced CTorrent Version Detection

Summary
This script retrieves CTorrent/Enhanced CTorrent version and saves the result in KB.

Vulnerability Detection Result
```
Detected CTorrent/Enhanced CTorrent
Version:  2
Location: /usr/bin/ctorrent
stderr
CPE:      cpe:/a:rahul:dtorrent:2
Concluded from version/product identification result:
2
```

Log Method
Details:CTorrent/Enhanced CTorrent Version Detection
OID:1.3.6.1.4.1.25623.1.0.900556
Version used: $Revision: 5943 $

Log (CVSS: 0.0)
NVT: Desktop Boards BIOS Information Detection for Linux

Summary
Detection of installed version of Desktop Boards BIOS.
The script logs in via ssh and queries for the version using the command line tool 'dmidecode'.
Usually this command requires root privileges to execute.

Vulnerability Detection Result
```
Desktop Boards BIOS version 6.00
stderr is not a tty - where are you? was detected on the host
Desktop Boards BIOS Vendor Phoenix Technologies LTD
stderr is not a tty - where are you? was detected on the host
Desktop Boards Base Board version None
stderr is not a tty - where are you? was detected on the host
Desktop Boards Base Board Manufacturer Intel Corporation
stderr is not a tty - where are you? was detected on the host
Desktop Boards Base Board Product Name 440BX Desktop Reference Platform
stderr is not a tty - where are you? was detected on the host
```

Log Method
Details:Desktop Boards BIOS Information Detection for Linux
OID:1.3.6.1.4.1.25623.1.0.800163
Version used: $Revision: 6032 $

Log (CVSS: 0.0)
NVT: Firewall Builder Version Detection (Linux)

Summary
This script detects the installed version of Firewall Builder and sets the result in KB.

Vulnerability Detection Result
```
Firewall Builder version 1 running at location /opt/kde/bin/fwbuilder
stderr  was detected on the host
```

Log Method
Details:`Firewall Builder Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800995
Version used: `$Revision: 2836 $`

Log (CVSS: 0.0)
NVT: Firewall Builder Version Detection (Linux)

Summary
This script detects the installed version of Firewall Builder and sets the result in KB.

Vulnerability Detection Result
```
Firewall Builder version . running at location tty  was detected on the host
```

Log Method
Details:`Firewall Builder Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800995
Version used: `$Revision: 2836 $`

Log (CVSS: 0.0)
NVT: FreeType Version Detection (Linux)

Summary
Detection of installed version of FreeType.
The script logs in via ssh, searches for executable 'freetype-config' and queries the found executables via command line option '–ftversion'.

Vulnerability Detection Result
```
Detected FreeType version: 2.2.1
Location: /usr/local/bin/freetype-config
CPE: cpe:/a:freetype:freetype:2.2.1
Concluded from version identification result:
2.2.1
stderr is not a tty - where are you?
```

Log Method

. . . continues on next page . . .

. . . continued from previous page . . .

Details:FreeType Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.900626
Version used: $Revision: 4487 $

Log (CVSS: 0.0)
NVT: FreeType Version Detection (Linux)

Summary
Detection of installed version of FreeType.
The script logs in via ssh, searches for executable 'freetype-config' and queries the found executables via command line option '–ftversion'.

Vulnerability Detection Result

```
Detected FreeType version: 2.1.10
Location: /usr/bin/freetype-config
CPE: cpe:/a:freetype:freetype:2.1.10
Concluded from version identification result:
2.1.10
stderr is not a tty - where are you?
```

Log Method
Details:FreeType Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.900626
Version used: $Revision: 4487 $

Log (CVSS: 0.0)
NVT: GD Graphics Library Version Detection (Linux)

Summary
This script detects the installed version of GD Graphics Library and sets the result in KB.

Vulnerability Detection Result

```
GD Graphics Library version .
 was detected on the host
```

Log Method
Details:GD Graphics Library Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.801121
Version used: $Revision: 6063 $

Log (CVSS: 0.0)
NVT: GD Graphics Library Version Detection (Linux)

Summary

. . . continues on next page . . .

... continued from previous page ...

This script detects the installed version of GD Graphics Library and sets the result in KB.

Vulnerability Detection Result

```
GD Graphics Library version 5.97
 was detected on the host
```

Log Method

Details:GD Graphics Library Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.801121
Version used: $Revision: 6063 $

Log (CVSS: 0.0)
NVT: GZip Version Detection (Linux)

Summary

Detection of installed version of GZip.
The script logs in via ssh, searches for executable 'gzip' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected GZip version: 1.3.5
Location: /bin/gzip
CPE: cpe:/a:gnu:gzip:1.3.5
Concluded from version identification result:
gzip 1.3.5
(2002-09-30)
Copyright 2002 Free Software Foundation
Copyright 1992-1993 Jean-loup Gailly
This program comes with ABSOLUTELY NO WARRANTY.
You may redistribute copies of this program
under the terms of the GNU General Public License.
For more information about these matters, see the file named COPYING.
Compilation options:
DIRENT UTIME STDC_HEADERS HAVE_UNISTD_H HAVE_MEMORY_H HAVE_STRING_H HAVE_LSTAT A
↪SMV
Written by Jean-loup Gailly.
stderr is not a tty - where are you?
```

Log Method

Details:GZip Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800450
Version used: $Revision: 5877 $

... continues on next page ...

... continued from previous page ...

Log (CVSS: 0.0)
NVT: ImageMagick version Detection (Linux)

Summary
Detection of installed version of ImageMagick on Linux.
The script logs in via ssh, searches for executable 'identify' and queries the found executables via command line option '-version'.

Vulnerability Detection Result

```
Detected ImageMagick
Version:  6.2.9
Location: /usr/local/bin/identify
stderr
CPE:      cpe:/a:imagemagick:imagemagick:6.2.9
Concluded from version/product identification result:
Version: ImageMagick 6.2.9 09/24/06 Q16 http://www.imagemagick.org
Copyright: Copyright (C) 1999-2006 ImageMagick Studio LLC
Usage: identify [options ...] file [ [options ...] file ... ]
Where options include:
  -antialias           remove pixel-aliasing
  -authenticate value  decrypt image with this password
  -channel type        apply option to select image channels
  -crop geometry       cut out a rectangular region of the image
  -debug events        display copious debugging information
  -define format:option
                       define one or more image format options
  -density geometry    horizontal and vertical density of the image
  -depth value         image depth
  -extract geometry    extract area from image
  -format "string"     output formatted image characteristics
  -fuzz distance       colors within this distance are considered equal
  -help                print program options
  -interlace type      type of image interlacing scheme
  -interpolate method  pixel color interpolation method
  -limit type value    pixel cache resource limit
  -list type           Color, Configure, Delegate, Format, Magic, Module,
                       Resource, or Type
  -log format          format of debugging information
  -matte               store matte channel if the image has one
  -monitor             monitor progress
  -ping                efficiently determine image attributes
  -quiet               suppress all error or warning messages
  -regard-warnings     pay attention to warning messages
  -sampling-factor geometry
                       horizontal and vertical sampling factor
  -set attribute value set an image attribute
  -size geometry       width and height of image
```

... continues on next page ...

... continued from previous page ...

```
  -strip               strip image of all profiles and comments
  -units type          the units of image resolution
  -verbose             print detailed information about the image
  -version             print version information
  -virtual-pixel method
                       virtual pixel access method
stderr is not a tty - where are you?
/bin/sh: line 1: stderr: command not found
```

Log Method
Details:ImageMagick version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.900563
Version used: $Revision: 3337 $

Log (CVSS: 0.0)
NVT: KDE Konqueror Version Detection

Summary
Detection of installed version of KDE Konqueror.
The script logs in via ssh, searches for executable 'konqueror' and queries the found executables via command line option '-v'.

Vulnerability Detection Result

```
Detected KDE Konqueror version: 3.5.3.Qt: 3.3.6
KDE: 3.5.3
Konqueror: 3.5.3
stderr is not a tty - where are you?
Location: /opt/kde/bin/konqueror
CPE: cpe:/a:kde:konqueror:3.5.3
Concluded from version identification result:
Qt: 3.3.6
KDE: 3.5.3
Konqueror: 3.5.3
stderr is not a tty - where are you?
```

Log Method
Details:KDE Konqueror Version Detection
OID:1.3.6.1.4.1.25623.1.0.900902
Version used: $Revision: 2833 $

Log (CVSS: 0.0)
NVT: Mozilla Firefox Version Detection (Linux)

Summary
This script finds the Mozilla Firefox installed version on Linux and save the version in KB.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Detected Firefox
Version:  2.0.0.4
Location: /opt/firefox/firefox
CPE:      cpe:/a:mozilla:firefox:2.0.0.4
Concluded from version/product identification result:
2.0.0.4
```

Log Method

Details:Mozilla Firefox Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800017
Version used: $Revision: 6063 $

Log (CVSS: 0.0)
NVT: Mutt Version Detection

Summary

Detection of installed version of Mutt.
The script logs in via ssh, searches for executable 'mutt' and queries the found executables via command line option '-v'.

Vulnerability Detection Result

```
Detected Mutt version: 1.4.2.2i
Location: /usr/bin/mutt
CPE: cpe:/a:mutt:mutt:1.4.2.2
Concluded from version identification result:
Mutt 1.4.2.2i (2006-07-14)
Copyright (C) 1996-2002 Michael R. Elkins and others.
Mutt comes with ABSOLUTELY NO WARRANTY; for details type ‘mutt -vv’.
Mutt is free software, and you are welcome to redistribute it
under certain conditions; type ‘mutt -vv’ for details.
System: Linux 2.6.20-BT-PwnSauce-NOSMP (i686) [using ncurses 5.5]
Compile options:
-DOMAIN
-DEBUG
-HOMESPOOL  -USE_SETGID  +USE_DOTLOCK  -DL_STANDALONE
+USE_FCNTL  -USE_FLOCK
+USE_POP  +USE_IMAP  -USE_GSS  +USE_SSL  -USE_SASL
+HAVE_REGCOMP  -USE_GNU_REGEX
+HAVE_COLOR  +HAVE_START_COLOR  +HAVE_TYPEAHEAD  +HAVE_BKGDSET
+HAVE_CURS_SET  +HAVE_META  +HAVE_RESIZETERM
+HAVE_PGP  -BUFFY_SIZE -EXACT_ADDRESS  -SUN_ATTACHMENT
+ENABLE_NLS  +LOCALES_HACK  -HAVE_WC_FUNCS  +HAVE_LANGINFO_CODESET  +HAVE_LANGIN
↪FO_YESEXPR
+HAVE_ICONV  -ICONV_NONTRANS  +HAVE_GETSID  +HAVE_GETADDRINFO
ISPELL="/usr/bin/ispell"
```

... continues on next page ...

... continued from previous page ...

```
SENDMAIL="/usr/sbin/sendmail"
MAILPATH="/var/spool/mail"
PKGDATADIR="/usr/share/mutt"
SYSCONFDIR="/etc/mutt"
EXECSHELL="/bin/sh"
-MIXMASTER
To contact the developers, please mail to <mutt-dev@mutt.org>.
To report a bug, please use the flea(1) utility.
stderr is not a tty - where are you?
```

Log Method
Details:`Mutt Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900675
Version used: `$Revision: 5877 $`

Log (CVSS: 0.0)
NVT: OpenSSL Version Detection (Linux)

Summary
Detection of installed version of OpenSSL.
The script logs in via ssh, searches for executable 'openssl' and queries the found executables via command line option 'version'.

Vulnerability Detection Result

```
Detected OpenSSL
Version:  0.9.8d
Location: /usr/bin/openssl
CPE:      cpe:/a:openssl:openssl:0.9.8d
Concluded from version/product identification result:
OpenSSL 0.9.8d 28 Sep 2006
stderr is not a tty - where are you?
```

Log Method
Details:`OpenSSL Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.800335
Version used: `$Revision: 2836 $`

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional informations which might help to improve the OS detection.

... continues on next page ...

... continued from previous page ...

If any of this information is wrong or could be improved please consider to report these to openvas-plugins@wald.intevation.org.

Vulnerability Detection Result

```
Best matching OS:
OS: Slackware 11.0
CPE: cpe:/o:slackware:slackware_linux:11.0
Found by NVT: 1.3.6.1.4.1.25623.1.0.50282 (Determine OS and list of installed pa
↪ckages via SSH login)
Concluded from SSH login
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Linux
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/1.3.37 (Unix) P
↪HP/4.4.4
OS: Linux 2.6.13 - 2.6.32
CPE: cpe:/o:linux:linux_kernel:2.6
Found by NVT: 1.3.6.1.4.1.25623.1.0.108021 (Nmap OS Identification (NASL wrapper
↪))
Concluded from Nmap TCP/IP fingerprinting:
OS details: Linux 2.6.13 - 2.6.32
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS: Linux Kernel
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint:
(100% confidence)
Linux Kernel
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to openvas-plugins@wald.intevation.org:
Banner: SSH-1.99-OpenSSH_4.4
Identified from: SSH banner on port 22/tcp
Banner: Server: CUPS/1.1
Identified from: HTTP Server banner on port 631/tcp
```

Log Method

Details:OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: $Revision: 5435 $

Log (CVSS: 0.0)
NVT: Pango Version Detection

Summary

... continues on next page ...

... continued from previous page ...

Detection of installed version of Pango.
The script logs in via ssh, searches for executable 'pango-view' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Pango version: ...
Location: /usr/bin/pango-view
stderr
CPE: cpe:/a:pango:pango:...
Concluded from version identification result:
stderr is not a tty - where are you?
Usage: pango-view [OPTION...] FILE
/bin/sh: line 1: stderr: command not found
```

Log Method

Details:Pango Version Detection
OID:1.3.6.1.4.1.25623.1.0.900643
Version used: $Revision: 5877 $

Log (CVSS: 0.0)
NVT: Pango Version Detection

Summary

Detection of installed version of Pango.
The script logs in via ssh, searches for executable 'pango-view' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Pango version: 5.97
Location: tty
CPE: cpe:/a:pango:pango:5.97
Concluded from version identification result:
tty (GNU coreutils) 5.97
Copyright (C) 2006 Free Software Foundation, Inc.
This is free software.  You may redistribute copies of it under the terms of
the GNU General Public License <http://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.
Written by David MacKenzie.
stderr is not a tty - where are you?
```

Log Method

Details:Pango Version Detection
OID:1.3.6.1.4.1.25623.1.0.900643
Version used: $Revision: 5877 $

Log (CVSS: 0.0)
NVT: PHP Version Detection (Linux, local)

Summary
This script finds the installed PHP version on Linux and saves the version in KB.

Vulnerability Detection Result
```
Detected PHP
Version:  4.4.4
Location: /usr/local/bin/php
CPE:      cpe:/a:php:php:4.4.4
Concluded from version/product identification result:
PHP 4.4.4
```

Log Method
Details:`PHP Version Detection (Linux, local)`
OID:1.3.6.1.4.1.25623.1.0.103592
Version used: `$Revision: 5158 $`

Log (CVSS: 0.0)
NVT: PostgreSQL Version Detection (Linux)

Summary
Detection of installed version of PostgreSQL.
The script logs in via ssh, searches for executable 'psql' and queries the found executables via command line option '–version'.

Vulnerability Detection Result
```
Detected PostgreSQL version: 8.1.4
Location: /usr/local/pgsql/bin/psql
CPE: cpe:/a:postgresql:postgresql:8.1.4
Concluded from version identification result:
psql (PostgreSQL) 8.1.4
contains support for command-line editing
stderr is not a tty - where are you?
```

Log Method
Details:`PostgreSQL Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900478
Version used: `$Revision: 6032 $`

Log (CVSS: 0.0)
NVT: ProFTPD Server Version Detection (Local)

Summary
This script detects the installed version of ProFTPD Server and saves the version in KB.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
Detected ProFTPD
Version:  1.3.0
Location: /usr/local/sbin/proftpd
CPE:      cpe:/a:proftpd:proftpd:1.3.0
Concluded from version/product identification result:
1.3.0
```

Log Method

Details:ProFTPD Server Version Detection (Local)
OID:1.3.6.1.4.1.25623.1.0.900506
Version used: $Revision: 4774 $

Log (CVSS: 0.0)
NVT: QEMU Version Detection (Linux)

Summary

Detection of installed version of QEMU.
The script logs in via ssh, searches for executable 'qemu' and queries the found executables via command line option '-help'.

Vulnerability Detection Result

```
Detected QEMI PC emulator version: 0.9.0
Location: /usr/local/bin/qemu
CPE: cpe:/a:qemu:qemu:0.9.0
Concluded from version identification result:
QEMU PC emulator version 0.9.0, Copyright (c) 2003-2007 Fabrice Bellard
usage: qemu [options] [disk_image]
'disk_image' is a raw hard image image for IDE hard disk 0
Standard options:
-M machine      select emulated machine (-M ? for list)
-fda/-fdb file  use 'file' as floppy disk 0/1 image
-hda/-hdb file  use 'file' as IDE hard disk 0/1 image
-hdc/-hdd file  use 'file' as IDE hard disk 2/3 image
-cdrom file     use 'file' as IDE cdrom image (cdrom is ide1 master)
-boot [a|c|d|n] boot on floppy (a), hard disk (c), CD-ROM (d), or network (n)
-snapshot       write to temporary files instead of disk image files
-no-quit        disable SDL window close capability
-no-fd-bootchk  disable boot signature checking for floppy disks
-m megs         set virtual RAM size to megs MB [default=128]
-smp n          set the number of CPUs to 'n' [default=1]
-nographic      disable graphical output and redirect serial I/Os to console
-k language     use keyboard layout (for example "fr" for French)
-audio-help     print list of audio drivers and their options
-soundhw c1,... enable audio support
                and only specified sound cards (comma separated list)
```

... continues on next page ...

... continued from previous page ...

```
                use -soundhw ? to get the list of supported cards
                use -soundhw all to enable all of them
-localtime      set the real time clock to local time [default=utc]
-full-screen    start in full screen
-win2k-hack     use it when installing Windows 2000 to avoid a disk full bug
-usb            enable the USB driver (will be the default soon)
-usbdevice name add the host or guest USB device 'name'
Network options:
-net nic[,vlan=n][,macaddr=addr][,model=type]
                create a new Network Interface Card and connect it to VLAN 'n'
-net user[,vlan=n][,hostname=host]
                connect the user mode network stack to VLAN 'n' and send
                hostname 'host' to DHCP clients
-net tap[,vlan=n][,fd=h][,ifname=name][,script=file]
                connect the host TAP network interface to VLAN 'n' and use
                the network script 'file' (default=/etc/qemu-ifup);
                use 'script=no' to disable script execution;
                use 'fd=h' to connect to an already opened TAP interface
-net socket[,vlan=n][,fd=h][,listen=[host]:port][,connect=host:port]
                connect the vlan 'n' to another VLAN using a socket connection
-net socket[,vlan=n][,fd=h][,mcast=maddr:port]
                connect the vlan 'n' to multicast maddr and port
-net none       use it alone to have zero network devices; if no -net option
                is provided, the default is '-net nic -net user'
-tftp prefix    allow tftp access to files starting with prefix [-net user]
-smb dir        allow SMB access to files in 'dir' [-net user]
-redir [tcp|udp]:host-port:[guest-host]:guest-port
                redirect TCP or UDP connections from host to guest [-net user]
Linux boot specific:
-kernel bzImage use 'bzImage' as kernel image
-append cmdline use 'cmdline' as kernel command line
-initrd file    use 'file' as initial ram disk
Debug/Expert options:
-monitor dev    redirect the monitor to char device 'dev'
-serial dev     redirect the serial port to char device 'dev'
-parallel dev   redirect the parallel port to char device 'dev'
-pidfile file   Write PID to 'file'
-S              freeze CPU at startup (use 'c' to start execution)
-s              wait gdb connection to port 1234
-p port         change gdb connection port
-d item1,...    output log to /tmp/qemu.log (use -d ? for a list of log items)
-hdachs c,h,s[,t]  force hard disk 0 physical geometry and the optional BIOS
                translation (t=none or lba) (usually qemu can guess them)
-L path         set the directory for the BIOS, VGA BIOS and keymaps
-kernel-kqemu   enable KQEMU full virtualization (default is user mode only)
-no-kqemu       disable KQEMU kernel module usage
-std-vga        simulate a standard VGA card with VESA Bochs Extensions
```

... continues on next page ...

... continued from previous page ...

```
                (default is CL-GD5446 PCI VGA)
-no-acpi        disable ACPI
-no-reboot      exit instead of rebooting
-loadvm file    start right away with a saved state (loadvm in monitor)
-vnc display    start a VNC server on display
-daemonize      daemonize QEMU after initializing
-option-rom rom load a file, rom, into the option ROM space
During emulation, the following keys are useful:
ctrl-alt-f      toggle full screen
ctrl-alt-n      switch to virtual console 'n'
ctrl-alt        toggle mouse and keyboard grab
When using -nographic, press 'ctrl-a h' to get some help.
stderr is not a tty - where are you?
```

Log Method
Details:`QEMU Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900969
Version used: `$Revision: 2833 $`

Log (CVSS: 0.0)
NVT: QEMU Version Detection (Linux)

Summary
Detection of installed version of QEMU.
The script logs in via ssh, searches for executable 'qemu' and queries the found executables via command line option '-help'.

Vulnerability Detection Result

```
Detected QEMI PC emulator version: 0.9.0
Location: /usr/bin/qemu
CPE: cpe:/a:qemu:qemu:0.9.0
Concluded from version identification result:
QEMU PC emulator version 0.9.0, Copyright (c) 2003-2007 Fabrice Bellard
usage: qemu [options] [disk_image]
'disk_image' is a raw hard image image for IDE hard disk 0
Standard options:
-M machine      select emulated machine (-M ? for list)
-fda/-fdb file  use 'file' as floppy disk 0/1 image
-hda/-hdb file  use 'file' as IDE hard disk 0/1 image
-hdc/-hdd file  use 'file' as IDE hard disk 2/3 image
-cdrom file     use 'file' as IDE cdrom image (cdrom is ide1 master)
-boot [a|c|d|n] boot on floppy (a), hard disk (c), CD-ROM (d), or network (n)
-snapshot       write to temporary files instead of disk image files
-no-quit        disable SDL window close capability
-no-fd-bootchk  disable boot signature checking for floppy disks
-m megs         set virtual RAM size to megs MB [default=128]
-smp n          set the number of CPUs to 'n' [default=1]
```

... continues on next page ...

... continued from previous page ...

```
-nographic      disable graphical output and redirect serial I/Os to console
-k language     use keyboard layout (for example "fr" for French)
-audio-help     print list of audio drivers and their options
-soundhw c1,... enable audio support
                and only specified sound cards (comma separated list)
                use -soundhw ? to get the list of supported cards
                use -soundhw all to enable all of them
-localtime      set the real time clock to local time [default=utc]
-full-screen    start in full screen
-win2k-hack     use it when installing Windows 2000 to avoid a disk full bug
-usb            enable the USB driver (will be the default soon)
-usbdevice name add the host or guest USB device 'name'
Network options:
-net nic[,vlan=n][,macaddr=addr][,model=type]
                create a new Network Interface Card and connect it to VLAN 'n'
-net user[,vlan=n][,hostname=host]
                connect the user mode network stack to VLAN 'n' and send
                hostname 'host' to DHCP clients
-net tap[,vlan=n][,fd=h][,ifname=name][,script=file]
                connect the host TAP network interface to VLAN 'n' and use
                the network script 'file' (default=/etc/qemu-ifup);
                use 'script=no' to disable script execution;
                use 'fd=h' to connect to an already opened TAP interface
-net socket[,vlan=n][,fd=h][,listen=[host]:port][,connect=host:port]
                connect the vlan 'n' to another VLAN using a socket connection
-net socket[,vlan=n][,fd=h][,mcast=maddr:port]
                connect the vlan 'n' to multicast maddr and port
-net none       use it alone to have zero network devices; if no -net option
                is provided, the default is '-net nic -net user'
-tftp prefix    allow tftp access to files starting with prefix [-net user]
-smb dir        allow SMB access to files in 'dir' [-net user]
-redir [tcp|udp]:host-port:[guest-host]:guest-port
                redirect TCP or UDP connections from host to guest [-net user]
Linux boot specific:
-kernel bzImage use 'bzImage' as kernel image
-append cmdline use 'cmdline' as kernel command line
-initrd file    use 'file' as initial ram disk
Debug/Expert options:
-monitor dev    redirect the monitor to char device 'dev'
-serial dev     redirect the serial port to char device 'dev'
-parallel dev   redirect the parallel port to char device 'dev'
-pidfile file   Write PID to 'file'
-S              freeze CPU at startup (use 'c' to start execution)
-s              wait gdb connection to port 1234
-p port         change gdb connection port
-d item1,...    output log to /tmp/qemu.log (use -d ? for a list of log items)
-hdachs c,h,s[,t]  force hard disk 0 physical geometry and the optional BIOS
```

... continues on next page ...

... continued from previous page ...

```
                translation (t=none or lba) (usually qemu can guess them)
-L path         set the directory for the BIOS, VGA BIOS and keymaps
-kernel-kqemu   enable KQEMU full virtualization (default is user mode only)
-no-kqemu       disable KQEMU kernel module usage
-std-vga        simulate a standard VGA card with VESA Bochs Extensions
                (default is CL-GD5446 PCI VGA)
-no-acpi        disable ACPI
-no-reboot      exit instead of rebooting
-loadvm file    start right away with a saved state (loadvm in monitor)
-vnc display    start a VNC server on display
-daemonize      daemonize QEMU after initializing
-option-rom rom load a file, rom, into the option ROM space
During emulation, the following keys are useful:
ctrl-alt-f      toggle full screen
ctrl-alt-n      switch to virtual console 'n'
ctrl-alt        toggle mouse and keyboard grab
When using -nographic, press 'ctrl-a h' to get some help.
stderr is not a tty - where are you?
```

Log Method
Details:`QEMU Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900969
Version used: `$Revision: 2833 $`

Log (CVSS: 0.0)
NVT: Ruby On Rails Version Detection

Summary
This script detect the installed version of Ruby On Rails and sets the result in KB.

Vulnerability Detection Result

```
Ruby On Rails version 1.2.2 running at location /usr/bin/rails
 was detected on the host
```

Log Method
Details:`Ruby On Rails Version Detection`
OID:1.3.6.1.4.1.25623.1.0.800911
Version used: `$Revision: 6063 $`

Log (CVSS: 0.0)
NVT: Ruby Version Detection (Linux)

Summary
Detection of installed version of Ruby.

... continues on next page ...

... continued from previous page ...

The script logs in via ssh, searches for executable 'ruby' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Ruby version: 1.8.4
Location: /usr/bin/ruby
CPE: cpe:/a:ruby-lang:ruby:1.8.4
Concluded from version identification result:
ruby 1.8.4 (2005-12-24) [i686-linux]
stderr is not a tty - where are you?
```

Log Method

Details:`Ruby Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900569
Version used: `$Revision: 2833 $`

Log (CVSS: 0.0)
NVT: Samba Version Detection

Summary

Detection of installed version of Samba.
The script logs in via ssh, searches for executable 'smbd' and queries the found executables via command line option '-V'.

Vulnerability Detection Result

```
Detected Samba
Version:  3.0.14a
Location: /usr/sbin/smbd
CPE:      cpe:/a:samba:samba:3.0.14
Concluded from version/product identification result:
stderr is not a tty - where are you?
```

Log Method

Details:`Samba Version Detection`
OID:1.3.6.1.4.1.25623.1.0.800403
Version used: `$Revision: 5886 $`

Log (CVSS: 0.0)
NVT: Snort Version Detection (Linux)

Summary

This script detects the installed version of Snort and sets the reuslt in KB.

Vulnerability Detection Result

```
Snort version 2.6.1.2.34 running at location /usr/local/bin/snort
```

... continues on next page ...

... continued from previous page ...

stderr was detected on the host

Log Method
Details:Snort Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.801138
Version used: $Revision: 6032 $

Log (CVSS: 0.0)
NVT: Subversion Version Detection

Summary
Detection of installed version of Subversion.
The script logs in via ssh, searches for executable 'svnversion' and queries the found executables via command line option '–version'.

Vulnerability Detection Result
Detected Subversion version: 1
Location: /usr/local/bin/svnversion
stderr
CPE: cpe:/a:subversion:subversion:1
Concluded from version identification result:
exported
stderr is not a tty - where are you?
/bin/sh: line 1: stderr: command not found

Log Method
Details:Subversion Version Detection
OID:1.3.6.1.4.1.25623.1.0.101103
Version used: $Revision: 2833 $

Log (CVSS: 0.0)
NVT: Subversion Version Detection

Summary
Detection of installed version of Subversion.
The script logs in via ssh, searches for executable 'svnversion' and queries the found executables via command line option '–version'.

Vulnerability Detection Result
Detected Subversion version: 5.97
Location: tty
CPE: cpe:/a:subversion:subversion:5.97
Concluded from version identification result:
tty (GNU coreutils) 5.97
Copyright (C) 2006 Free Software Foundation, Inc.

... continues on next page ...

... continued from previous page ...

```
This is free software.  You may redistribute copies of it under the terms of
the GNU General Public License <http://www.gnu.org/licenses/gpl.html>.
There is NO WARRANTY, to the extent permitted by law.
Written by David MacKenzie.
stderr is not a tty - where are you?
```

Log Method
Details:Subversion Version Detection
OID:1.3.6.1.4.1.25623.1.0.101103
Version used: $Revision: 2833 $

Log (CVSS: 0.0)
NVT: Sun Java Products Version Detection (Linux)

Summary
Detection of installed version of Java products on Linux systems. It covers Sun Java, IBM Java and GCJ.
The script logs in via ssh, searches for executables 'javaaws' and 'java' and queries the found executables via command line option '-fullversion'.

Vulnerability Detection Result

```
Detected Sun Java JRE
Version:  1.5.0_06-b05
Location: /usr/lib/java/bin/java
CPE:      cpe:/a:sun:jre:1.5.0_06
Concluded from version/product identification result:
1.5.0_06-b05
```

Log Method
Details:Sun Java Products Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800385
Version used: $Revision: 5943 $

Log (CVSS: 0.0)
NVT: Sun Java Products Version Detection (Linux)

Summary
Detection of installed version of Java products on Linux systems. It covers Sun Java, IBM Java and GCJ.
The script logs in via ssh, searches for executables 'javaaws' and 'java' and queries the found executables via command line option '-fullversion'.

Vulnerability Detection Result

```
Detected Sun Java JRE
Version:  1.5.0_06-b05
```

... continues on next page ...

... continued from previous page ...

```
Location: /usr/lib/java/jre/bin/java
CPE:      cpe:/a:sun:jre:1.5.0_06
Concluded from version/product identification result:
1.5.0_06-b05
```

Log Method
Details:Sun Java Products Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.800385
Version used: $Revision: 5943 $

Log (CVSS: 0.0)
NVT: Tor Version Detection (Linux)

Summary
Detection of installed version of Tor.
The script logs in via ssh, searches for executable 'tor' and queries the found executables via command line option '–version'.

Vulnerability Detection Result

```
Detected Tor
Version:  0.1.1.26.
Location: /usr/local/bin/tor
CPE:      cpe:/a:tor:tor:0.1.1.26.
Concluded from version/product identification result:
0.1.1.26.
```

Log Method
Details:Tor Version Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.900418
Version used: $Revision: 2725 $

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 192.168.27.32 to 192.168.27.45:
192.168.27.32
192.168.27.45
```

... continues on next page ...

... continued from previous page ...

Solution
Block unwanted packets from escaping your network.

Log Method
Details:`Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `$Revision: 5390 $`

Log (CVSS: 0.0)
NVT: VLC Media Player Version Detection (Linux)

Summary
Detection of installed version of VLC Media Player version on Linux.
This script logs in via shh, extracts the version from the binary file and set it in KB.

Vulnerability Detection Result
```
Detected VLC Media Player
Version:  0.8.4a
Location: /usr/bin/vlc
CPE:      cpe:/a:videolan:vlc_media_player:0.8.4a:a
Concluded from version/product identification result:
0.8.4a
```

Log Method
Details:`VLC Media Player Version Detection (Linux)`
OID:1.3.6.1.4.1.25623.1.0.900529
Version used: `$Revision: 2636 $`

Log (CVSS: 0.0)
NVT: WebDAV Neon Version Detection

Summary
This script detects the installed version of WebDAV Neon and sets the reuslt in KB.

Vulnerability Detection Result
```
WebDAV Neon version 0.25.5 was detected on the host
```

Log Method
Details:`WebDAV Neon Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900827
Version used: `$Revision: 5877 $`

... continues on next page ...

. . . continued from previous page . . .

Log (CVSS: 10.0)
NVT: X Server

Summary
This plugin detects X Window servers.
X11 is a client - server protocol. Basically, the server is in charge of the screen, and the clients connect to it and send several requests like drawing a window or a menu, and the server sends events back to the clients, such as mouse clicks, key strokes, and so on...
An improperly configured X server will accept connections from clients from anywhere. This allows an attacker to make a client connect to the X server to record the keystrokes of the user, which may contain sensitive information, such as account passwords. This can be prevented by using xauth, MIT cookies, or preventing the X server from listening on TCP (a Unix sock is used for local connections)

Vulnerability Detection Result
```
Detected X Windows Server
Version:  11.0
Location: undefined
CPE:      cpe:/a:x.org:x11:11.0
Concluded from version/product identification result:
11.0
```

Vulnerability Detection Method
Details:`X Server`
OID:1.3.6.1.4.1.25623.1.0.10407
Version used: `$Revision: 5943 $`

References
`CVE: CVE-1999-0526`

Log (CVSS: 10.0)
NVT: X Server

Summary
This plugin detects X Window servers.
X11 is a client - server protocol. Basically, the server is in charge of the screen, and the clients connect to it and send several requests like drawing a window or a menu, and the server sends events back to the clients, such as mouse clicks, key strokes, and so on...
An improperly configured X server will accept connections from clients from anywhere. This allows an attacker to make a client connect to the X server to record the keystrokes of the user, which may contain sensitive information, such as account passwords. This can be prevented by using xauth, MIT cookies, or preventing the X server from listening on TCP (a Unix sock is used for local connections)

Vulnerability Detection Result
```
Detected X Windows Server
```

. . . continues on next page . . .

... continued from previous page ...

```
Version:  11.0
Location: undefined
CPE:      cpe:/a:x.org:x11:11.0
Concluded from version/product identification result:
11.0
```

Vulnerability Detection Method
Details:X Server
OID:1.3.6.1.4.1.25623.1.0.10407
Version used: $Revision: 5943 $

References
CVE: CVE-1999-0526

Log (CVSS: 0.0)
NVT: Xpdf Version Detection

Summary
The PDF viewer Xpdf is installed and its version is detected.

Vulnerability Detection Result

```
Detected Xpdf version: 3.01
Location: /usr/local/bin/xpdf
CPE: cpe:/a:foolabs:xpdf:3.01
Concluded from version identification result:
stderr is not a tty - where are you?
/usr/local/bin/xpdf: Symbol `_XmStrings' has different size in shared object, co
↪nsider re-linking
xpdf version 3.01
Copyright 1996-2005 Glyph & Cog, LLC
```

Affected Software/OS
Xpdf on Linux.

Log Method
The script logs in via ssh, searches for executable 'xpdf' and queries the found executables via command line option '-v'.
Details:Xpdf Version Detection
OID:1.3.6.1.4.1.25623.1.0.900466
Version used: $Revision: 5877 $

[return to 192.168.27.45]

2.1.13 Log 6001/tcp

Log (CVSS: 0.0)
NVT: Identify Unknown Services with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.

Vulnerability Detection Result
`Nmap service detection result for this port: X11`

Log Method
Details:`Identify Unknown Services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5296 $`

[return to 192.168.27.45]

2.1.14 Log 69/udp

Log (CVSS: 0.0)
NVT: TFTP detection

Summary
The remote host has a TFTP server running. TFTP stands for Trivial File Transfer Protocol.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Disable TFTP server if not used.

Log Method
Details:`TFTP detection`
OID:1.3.6.1.4.1.25623.1.0.80100
Version used: `$Revision: 5515 $`

[return to 192.168.27.45]

2.1.15 Log 22/tcp

Log (CVSS: 0.0)
NVT: Determine OS and list of installed packages via SSH login

Summary

. . . continues on next page . . .

... continued from previous page ...

This script will, if given a userid/password or key to the remote system, login to that system, determine the OS it is running, and for supported systems, extract the list of installed packages/rpms.

Vulnerability Detection Result
`We are able to login and detect that you are running Slackware 11.0`

Vulnerability Insight
The ssh protocol is used to log in. If a specific port is configured for the credential, then only this port will be tried. Else any port that offers ssh, usually port 22.
Upon successful login, the command 'uname -a' is issued to find out about the type and version of the operating system.
The result is analysed for various patterns and in several cases additional commands are tried to find out more details and to confirm a detection.
The regular Linux distributions are detected this way as well as other linunxoid systems and also many Linux-baseddevices and appliances.
If the system offers a package database, for example RPM- or DEB-based, this full list of installed packages is retrieved for further patch-level checks.

Log Method
Details:`Determine OS and list of installed packages via SSH login`
OID:1.3.6.1.4.1.25623.1.0.50282
Version used: `$Revision: 6011 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`An ssh server is running on this port`

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 5180 $`

Log (CVSS: 0.0)
NVT: SSH Authorization Check

Summary
This script tries to login with provided credentials.

... continues on next page ...

... continued from previous page ...

If the login was successful, it marks this port as available for any authenticated tests.

Vulnerability Detection Result

```
It was possible to login using the provided SSH credentials.
Hence authenticated checks are enabled.
```

Log Method

Details:SSH Authorization Check
OID:1.3.6.1.4.1.25623.1.0.90022
Version used: $Revision: 5462 $

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary

This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-h
↪ellman-group14-sha1,diffie-hellman-group1-sha1
server_host_key_algorithms:
ssh-rsa,ssh-dss
encryption_algorithms_client_to_server:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
encryption_algorithms_server_to_client:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
mac_algorithms_client_to_server:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-m
↪d5-96
mac_algorithms_server_to_client:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-m
↪d5-96
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Log Method

Details:SSH Protocol Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: $Revision: 2828 $

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result
```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
1.5
2.0
1.33
SSHv1 Fingerprint: 6a:2b:e4:53:78:97:55:0e:72:a6:d4:c4:44:d0:bb:8b
SSHv2 Fingerprint:
ssh-dss: 63:2a:ef:f2:07:82:65:a7:4c:07:23:b2:02:52:e6:3c
ssh-rsa: 9e:a2:45:d7:65:0b:ed:6b:0d:ad:7f:d2:51:8b:0b:5a
```

Log Method
Details:`SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `$Revision: 4484 $`

Log (CVSS: 0.0)
NVT: SSH Server type and version

Summary
This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result
```
Detected SSH server version: SSH-1.99-OpenSSH_4.4
Remote SSH supported authentication: password,publickey,keyboard-interactive
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:4.4
Concluded from remote connection attempt with credentials:
  Login: VulnScan
  Password: VulnScan
```

Log Method
Details:`SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `$Revision: 4947 $`

[return to 192.168.27.45]

2.1.16 Log 5801/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use

Vulnerability Detection Result
```
Requests to this service are done via HTTP/1.0.
This service seems to be NOT able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The following directories were used for CGI scanning:
http://192.168.27.45:5801/
http://192.168.27.45:5801/cgi-bin
http://192.168.27.45:5801/scripts
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details:`CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `$Revision: 5907 $`

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

Summary
This script uses DIRB to find directories and files on web applications via brute forcing. See the preferences section for configuration options.

Vulnerability Detection Result
```
This are the directories/files found with brute force:
http://192.168.27.45:5801/
```

Log Method
Details:`DIRB (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: `$Revision: 4685 $`

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

Summary
This plugin uses nikto(1) to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.

Vulnerability Detection Result

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ No web server found on 192.168.27.45:5801
---------------------------------------------------------------------------
+ 0 host(s) tested
```

Log Method
Details:Nikto (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: $Revision: 4685 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
A web server is running on this port
```

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 5180 $

[return to 192.168.27.45]

2.1.17 Log 3306/tcp

Log (CVSS: 0.0)
NVT: MySQL/MariaDB Detection

Summary
Detection of installed version of MySQL/MariaDB.

. . . continues on next page . . .

... continued from previous page ...

Detect a running MySQL/MariaDB by getting the banner, Extract the version from the banner and store the information in KB

Vulnerability Detection Result

```
Detected MySQL
Version:  unknown
Location: 3306/tcp
CPE:      cpe:/a:oracle:mysql
Concluded from version/product identification result:
unknown
Scanner received a ER_HOST_NOT_PRIVILEGED error from the remote MySQL server.
Some tests may fail. Allow the scanner to access the remote MySQL server for bet
↪ter results.
```

Log Method

Details:`MySQL/MariaDB Detection`
OID:1.3.6.1.4.1.25623.1.0.100152
Version used: `$Revision: 5235 $`

Log (CVSS: 0.0)
NVT: Services

Summary

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
A MySQL server is running on this port
```

Log Method

Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 5180 $`

[return to 192.168.27.45]

2.1.18 Log 5901/tcp

Log (CVSS: 0.0)
NVT: VNC security types

Summary

This script checks the remote VNC protocol version and the available 'security types'.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
The remote VNC server supports those security types:
+ 2 (VNC authentication)
+ 16 (Tight)

Log Method
Details:VNC security types
OID:1.3.6.1.4.1.25623.1.0.19288
Version used: $Revision: 4469 $

Log (CVSS: 0.0)
NVT: VNC Server and Protocol Version Detection

Summary
The remote host is running a remote display software (VNC) which permits a console to be displayed remotely.
This allows authenticated users of the remote host to take its control remotely.

Vulnerability Detection Result
A VNC server seems to be running on this port.
The version of the VNC protocol is : RFB 003.007

Solution
Make sure the use of this software is done in accordance with your corporate security policy, filter incoming traffic to this port.

Log Method
Details:VNC Server and Protocol Version Detection
OID:1.3.6.1.4.1.25623.1.0.10342
Version used: $Revision: 4944 $

[return to 192.168.27.45]

2.1.19 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Log Method
Details:`ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 5309 $`

References
`CVE: CVE-1999-0524`
`Other:`
`URL:http://www.ietf.org/rfc/rfc0792.txt`

Log (CVSS: 0.0)
NVT: Record route

Summary
This plugin sends packets with the 'Record Route' option. It is a complement to traceroute.

Vulnerability Detection Result
```
Here is the route recorded between 192.168.27.32 and 192.168.27.45 :
192.168.27.45.
192.168.27.45.
```

Log Method
Details:`Record route`
OID:1.3.6.1.4.1.25623.1.0.12264
Version used: `$Revision: 6056 $`

[return to 192.168.27.45]

2.1.20 Log 631/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Requests to this service are done via HTTP/1.1.
This service seems to be NOT able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The following directories were used for CGI scanning:
http://192.168.27.45:631/
http://192.168.27.45:631/cgi-bin
http://192.168.27.45:631/scripts
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details:`CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `$Revision: 5907 $`

Log (CVSS: 0.0)
NVT: CUPS Version Detection

Summary
Detection of installed version of Common Unix Printing System (CUPS)
This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.

Vulnerability Detection Result

```
Detected CUPS
Version:  1.1
Location: /
CPE:      cpe:/a:apple:cups:1.1
Concluded from version/product identification result:
Server: CUPS/1.1
```

Log Method
Details:`CUPS Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900348
Version used: `$Revision: 6040 $`

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

Summary
This script uses DIRB to find directories and files on web applications via brute forcing. See the preferences section for configuration options.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
This are the directories/files found with brute force:
http://192.168.27.45:5801/
http://192.168.27.45:631/
```

Log Method
Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: $Revision: 4685 $

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result

```
The remote web server type is :
CUPS/1.1
```

Solution
Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method
Details:HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: $Revision: 5943 $

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

Summary
This plugin uses nikto(1) to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.

Vulnerability Detection Result

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.27.45
+ Target Hostname:    192.168.27.45
+ Target Port:        631
+ Start Time:         2017-05-26 13:40:11 (GMT0)
---------------------------------------------------------------------------
```

... continues on next page ...

... continued from previous page ...

```
+ Server: CUPS/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
↪gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
↪to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, POST, PUT
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to s
↪ave files on the web server.
+ 26191 requests: 1 error(s) and 5 item(s) reported on remote host
+ End Time:           2017-05-26 13:41:40 (GMT0) (89 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Log Method
Details:Nikto (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: $Revision: 4685 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A web server is running on this port

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 5180 $

[return to 192.168.27.45]

2.1.21 Log 5001/tcp

Log (CVSS: 0.0)
NVT: Identify Unknown Services with nmap

Summary

... continues on next page ...

... continued from previous page ...

This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.

Vulnerability Detection Result
`Nmap service detection result for this port: java-rmi`

Log Method
Details:`Identify Unknown Services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5296 $`

[return to 192.168.27.45]

2.1.22 Log 80/tcp

Log (CVSS: 0.0)
NVT: Apache Web Server Version Detection

Summary
Detection of installed version of Apache Web Server
The script detects the version of Apache HTTP Server on remote host and sets the KB.

Vulnerability Detection Result
```
Detected Apache
Version:  1.3.37
Location: 80/tcp
CPE:      cpe:/a:apache:http_server:1.3.37
Concluded from version/product identification result:
Server: Apache/1.3.37
```

Log Method
Details:`Apache Web Server Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900498
Version used: `$Revision: 4249 $`

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The following directories were used for CGI scanning:
http://192.168.27.45/
http://192.168.27.45/base
http://192.168.27.45/beef
http://192.168.27.45/beef/hook
http://192.168.27.45/beef/include
http://192.168.27.45/beef/modules
http://192.168.27.45/beef/modules/alert
http://192.168.27.45/beef/modules/browser
http://192.168.27.45/beef/modules/clipboard
http://192.168.27.45/beef/modules/portscanner
http://192.168.27.45/beef/modules/request
http://192.168.27.45/beef/tmp
http://192.168.27.45/beef/tmp/de2dfc7a9a4bfd754ffd38a21373c091
http://192.168.27.45/beef/ui
http://192.168.27.45/cgi-bin
http://192.168.27.45/docs
http://192.168.27.45/info
http://192.168.27.45/manual
http://192.168.27.45/manual/howto
http://192.168.27.45/manual/misc
http://192.168.27.45/manual/mod
http://192.168.27.45/manual/programs
http://192.168.27.45/manual/vhosts
http://192.168.27.45/olate
http://192.168.27.45/olate/templates/olate
http://192.168.27.45/olate/templates/olate/global
http://192.168.27.45/phpmyadmin
http://192.168.27.45/scripts
http://192.168.27.45/unicornscan
http://192.168.27.45/webexploitation_package_01
http://192.168.27.45/webexploitation_package_01/exploitme001
http://192.168.27.45/webexploitation_package_01/exploitme002
http://192.168.27.45/webexploitation_package_01/exploitme003
http://192.168.27.45/webexploitation_package_01/exploitme004
http://192.168.27.45/webexploitation_package_01/exploitme005
http://192.168.27.45/webexploitation_package_02
http://192.168.27.45/webexploitation_package_02/board51
http://192.168.27.45/webexploitation_package_02/board51/boarddata
http://192.168.27.45/webexploitation_package_02/board51/solution
http://192.168.27.45/webexploitation_package_02/cyphor
http://192.168.27.45/webexploitation_package_02/e107
http://192.168.27.45/webexploitation_package_02/iseasynews
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.27.45/webexploitation_package_02/isguestbook
http://192.168.27.45/webexploitation_package_02/isguestbook/smileys
http://192.168.27.45/webexploitation_package_02/isshout
http://192.168.27.45/webexploitation_package_02/isshout/admin
http://192.168.27.45/webexploitation_package_02/isshout/smileys
http://192.168.27.45/webexploitation_package_02/isshout/templates/default/
http://192.168.27.45/webexploitation_package_02/joomla107
http://192.168.27.45/webexploitation_package_02/joomla107/administrator
http://192.168.27.45/webexploitation_package_02/joomla109
http://192.168.27.45/webexploitation_package_02/nabopoll
http://192.168.27.45/webexploitation_package_02/nabopoll/admin
http://192.168.27.45/webexploitation_package_02/nabopoll/includes
http://192.168.27.45/webexploitation_package_02/nabopoll/templates
http://192.168.27.45/webexploitation_package_02/nabopoll/test
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13
http://192.168.27.45/webexploitation_package_02/phpforum_notworking
http://192.168.27.45/webexploitation_package_02/phpnuke7.4
http://192.168.27.45/webexploitation_package_02/phpnuke7.8
http://192.168.27.45/webexploitation_package_02/phpnuke7.8/includes/tiny_mce
http://192.168.27.45/webexploitation_package_02/solutions
http://192.168.27.45/webexploitation_package_02/webnews
http://192.168.27.45/webexploitation_package_02/webnews/design
http://192.168.27.45/webexploitation_package_02/wordpress
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because of the "Regex
↪pattern to exclude directories from CGI scanning" setting of the NVT "Global v
↪ariable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288):
http://192.168.27.45/beef/css
http://192.168.27.45/beef/images
http://192.168.27.45/beef/js
http://192.168.27.45/icons
http://192.168.27.45/manual/images
http://192.168.27.45/olate/templates/olate/images
http://192.168.27.45/phpmyadmin/css
http://192.168.27.45/phpmyadmin/themes/original/img
http://192.168.27.45/webexploitation_package_02/isshout/templates/default//image
↪s
http://192.168.27.45/webexploitation_package_02/nabopoll/images
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/templates/subSilve
↪r/images
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/templates/subSilve
↪r/images
http://192.168.27.45/webexploitation_package_02/phpnuke7.4/images
http://192.168.27.45/webexploitation_package_02/phpnuke7.4/images/powered
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.27.45/webexploitation_package_02/phpnuke7.4/themes/DeepBlue/image
↪s
http://192.168.27.45/webexploitation_package_02/phpnuke7.4/themes/DeepBlue/style
http://192.168.27.45/webexploitation_package_02/phpnuke7.8/images
http://192.168.27.45/webexploitation_package_02/phpnuke7.8/images/powered
http://192.168.27.45/webexploitation_package_02/phpnuke7.8/themes/DeepBlue/image
↪s
http://192.168.27.45/webexploitation_package_02/phpnuke7.8/themes/DeepBlue/style
Directory index found at:
http://192.168.27.45/
http://192.168.27.45/beef/
http://192.168.27.45/beef/css/
http://192.168.27.45/beef/images/
http://192.168.27.45/beef/include/
http://192.168.27.45/beef/js/
http://192.168.27.45/beef/modules/
http://192.168.27.45/beef/tmp/
http://192.168.27.45/webexploitation_package_01/
http://192.168.27.45/webexploitation_package_02/
http://192.168.27.45/webexploitation_package_02/board51/
http://192.168.27.45/webexploitation_package_02/iseasynews/
http://192.168.27.45/webexploitation_package_02/nabopoll/
http://192.168.27.45/webexploitation_package_02/solutions/
Extraneous phpinfo() script found at:
http://192.168.27.45/info.php
http://192.168.27.45/webexploitation_package_01/info.php
PHP script discloses physical path at:
http://192.168.27.45/unicornscan/ (/usr/local/apache/htdocs/unicornscan/lib/pgsq
↪ldbclass.php)
http://192.168.27.45/unicornscan/?D=A (/usr/local/apache/htdocs/unicornscan/lib/
↪pgsqldbclass.php)
http://192.168.27.45/webexploitation_package_02/phpforum_notworking/ (/usr/local
↪/apache/htdocs/webexploitation_package_02/phpforum_notworking/head.php)
http://192.168.27.45/webexploitation_package_02/phpforum_notworking/?D=A (/usr/l
↪ocal/apache/htdocs/webexploitation_package_02/phpforum_notworking/head.php)
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://192.168.27.45/ (D [A] M [A] N [D] S [A] )
http://192.168.27.45/beef/ (D [A] M [A] N [D] D=D [] S [A] )
http://192.168.27.45/beef/css/ (D [A] M [A] N [D] S [A] )
http://192.168.27.45/beef/images/ (D [A] M [A] N [D] S [A] )
http://192.168.27.45/beef/include/ (D [A] M [A] N [D] D=D [] S [A] )
http://192.168.27.45/beef/js/ (D [A] M [A] N [D] S [A] )
http://192.168.27.45/beef/modules/ (D [A] M [A] N [D] D=D [] S [A] )
http://192.168.27.45/beef/tmp/ (D [A] M [A] N [D] D=D [] S [A] )
http://192.168.27.45/info.php (0 [PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000] 0 [PH
↪PE9568F34-D428-11d2-A769-00AA001ACF42] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.27.45/manual/howto/ (M [A] N [A] D=D [] S [A] )
http://192.168.27.45/olate/details.php (file [43] )
http://192.168.27.45/olate/download.php (file [43] )
http://192.168.27.45/olate/files.php (cat [2] )
http://192.168.27.45/olate/index.php (cmd [top] )
http://192.168.27.45/olate/search.php (query [] )
http://192.168.27.45/olate/templates/olate/global/ (M [A] N [A] D=D [] S [A] )
http://192.168.27.45/olate/userupload.php (mirror3_name [] mirror5_url [] mirror
↪5_location [] mirror5_name [] submit [1] mirror4_url [] mirror3_location [] mi
↪rror3_url [] mirror1_location [] size [] mirror2_url [] convert_newlines [0] m
↪irror1_url [] name [] category [] mirror2_name [] upload [1] mirror4_name [] m
↪irror4_location [] mirror2_location [] filesize_format [] cmd [files_add_file]
↪ mirror1_name [] )
http://192.168.27.45/phpmyadmin/css/phpmyadmin.css.php (token [d8727bb48ca22db34
↪621bb079ca42cd5] collation_connection [utf8_unicode_ci] js_frame [right] lang
↪[en-utf-8] nocache [1495801315] convcharset [iso-8859-1] )
http://192.168.27.45/phpmyadmin/index.php (pma_username [] table [] collation_co
↪nnection [utf8_unicode_ci] lang [] server [1] db [] convcharset [iso-8859-1] p
↪ma_password [] )
http://192.168.27.45/webexploitation_package_01/ (D [A] M [A] N [D] D=D [] S [A]
↪ )
http://192.168.27.45/webexploitation_package_01/exploitme001/reset.php (email []
↪ user [DumbUser] )
http://192.168.27.45/webexploitation_package_01/exploitme002/reset.php (email []
↪ user [DumbUser] )
http://192.168.27.45/webexploitation_package_01/exploitme003/upload.php (MAX_FIL
↪E_SIZE [1024] attachment [] )
http://192.168.27.45/webexploitation_package_01/exploitme004/comment.php (name [
↪] )
http://192.168.27.45/webexploitation_package_01/exploitme005/buy.php (item [] qu
↪antity [] )
http://192.168.27.45/webexploitation_package_01/info.php (0 [PHPB8B5F2A0-3C92-11
↪d3-A3A9-4C7B08C10000] 0 [PHPE9568F34-D428-11d2-A769-00AA001ACF42] )
http://192.168.27.45/webexploitation_package_02/ (D [A] M [A] N [D] D=D [] S [A]
↪ )
http://192.168.27.45/webexploitation_package_02/board51/ (D [A] M [A] N [D] D=D
↪[] S [A] )
http://192.168.27.45/webexploitation_package_02/cyphor/index.php (submit [Login]
↪ pass [] login [] f_cookies [] )
http://192.168.27.45/webexploitation_package_02/cyphor/search.php (query_field [
↪] submit [Search] query_str [] query_discussion [] )
http://192.168.27.45/webexploitation_package_02/iseasynews/ (D [A] M [A] N [D] D
↪=D [] S [A] )
http://192.168.27.45/webexploitation_package_02/isguestbook/post.php (Submit [Su
↪bmit] Reset [Reset] name [] url [] email [] )
http://192.168.27.45/webexploitation_package_02/isshout/shout.php (message [] ur
↪l [] nom [] shout! [Shout!] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.27.45/webexploitation_package_02/joomla107/index.php (voteid [6]
↪remember [yes] Submit [Login] searchword [search...] bid [1] task [section] id
↪ [1] Itemid [3] username [] message [0] op2 [login] return [/webexploitation_p
↪ackage_02/joomla107/] feed [RSS0.91] no_html [1] lang [english] option [com_co
↪ntact] sectionid [3] task_button [Vote] passwd [] )
http://192.168.27.45/webexploitation_package_02/joomla109/index.php (searchword
↪[search...] Itemid [5] option [com_search] )
http://192.168.27.45/webexploitation_package_02/nabopoll/ (D [A] M [A] N [D] D=D
↪ [] S [A] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/faq.php (sid [edf6
↪bb81091fd0cc2426c8565bcd7933] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/groupcp.php (sid [
↪edf6bb81091fd0cc2426c8565bcd7933] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/index.php (sid [ed
↪f6bb81091fd0cc2426c8565bcd7933] c [1] mark [forums] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/login.php (passwor
↪d [] sid [edf6bb81091fd0cc2426c8565bcd7933] autologin [] login [Log in] userna
↪me [] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/memberlist.php (si
↪d [edf6bb81091fd0cc2426c8565bcd7933] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/privmsg.php (sid [
↪edf6bb81091fd0cc2426c8565bcd7933] folder [inbox] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/profile.php (sid [
↪edf6bb81091fd0cc2426c8565bcd7933] mode [register] u [2] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/search.php (sid [e
↪df6bb81091fd0cc2426c8565bcd7933] search_id [unanswered] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/viewforum.php (f [
↪1] sid [edf6bb81091fd0cc2426c8565bcd7933] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/viewonline.php (si
↪d [edf6bb81091fd0cc2426c8565bcd7933] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/viewtopic.php (sid
↪ [edf6bb81091fd0cc2426c8565bcd7933] p [1] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/faq.php (sid [9469
↪435ae7e7607ccbb97f38dd91fff1] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/groupcp.php (sid [
↪9469435ae7e7607ccbb97f38dd91fff1] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/index.php (sid [94
↪69435ae7e7607ccbb97f38dd91fff1] c [1] mark [forums] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/login.php (passwor
↪d [] sid [9469435ae7e7607ccbb97f38dd91fff1] autologin [] login [Log in] userna
↪me [] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/memberlist.php (si
↪d [9469435ae7e7607ccbb97f38dd91fff1] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/privmsg.php (sid [
↪9469435ae7e7607ccbb97f38dd91fff1] folder [inbox] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/profile.php (sid [
↪9469435ae7e7607ccbb97f38dd91fff1] mode [register] u [2] )
```

... continues on next page ...

... continued from previous page ...

```
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/search.php (sid [9
↪469435ae7e7607ccbb97f38dd91fff1] search_id [unanswered] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/viewforum.php (f [
↪1] sid [9469435ae7e7607ccbb97f38dd91fff1] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/viewonline.php (si
↪d [9469435ae7e7607ccbb97f38dd91fff1] )
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/viewtopic.php (sid
↪ [9469435ae7e7607ccbb97f38dd91fff1] p [1] )
http://192.168.27.45/webexploitation_package_02/phpnuke7.4/index.php (newlanguag
↪e [] )
http://192.168.27.45/webexploitation_package_02/phpnuke7.4/modules.php (thold []
↪ random_num [266661] gfx_check [] forwarder [modules.php?name=Surveys&amp;op=r
↪esults&amp;pollID=1] voteID [5] user_password [] name [Your_Account] pollID [1
↪] username [] order [] mode [] op [new_user] )
http://192.168.27.45/webexploitation_package_02/phpnuke7.8/index.php (newlanguag
↪e [] )
http://192.168.27.45/webexploitation_package_02/phpnuke7.8/modules.php (thold []
↪ random_num [961222] gfx_check [] voteID [5] user_password [] name [Your_Accou
↪nt] username [] pollID [1] order [] mode [] op [new_user] )
http://192.168.27.45/webexploitation_package_02/solutions/ (D [A] M [A] N [D] D=
↪D [] S [A] )
http://192.168.27.45/webexploitation_package_02/webnews/index.php (action [login
↪] name [] pw [] logintime [30] )
http://192.168.27.45/webexploitation_package_02/wordpress/index.php (s [] )
The following cgi scripts were excluded from CGI scanning because of the "Regex
↪pattern to exclude cgi scripts" setting of the NVT "Web mirroring" (OID: 1.3.6
↪.1.4.1.25623.1.0.10662):
Syntax : cginame (arguments [default value])
http://192.168.27.45/phpmyadmin/css/print.css (token [d8727bb48ca22db34621bb079c
↪a42cd5] collation_connection [utf8_unicode_ci] lang [en-utf-8] convcharset [is
↪o-8859-1] )
```

Log Method
Details:CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 5907 $

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

Summary
This script uses DIRB to find directories and files on web applications via brute forcing. See the preferences section for configuration options.

Vulnerability Detection Result

```
This are the directories/files found with brute force:
http://192.168.27.45:5801/
```

... continues on next page ...

... continued from previous page ...

http://192.168.27.45:80/

Log Method
Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: $Revision: 4685 $

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

Summary
This script uses DIRB to find directories and files on web applications via brute forcing. See the preferences section for configuration options.

Vulnerability Detection Result
This are the directories/files found with brute force:
http://192.168.27.45:5801/
http://192.168.27.45:631/
http://192.168.27.45:80/

Log Method
Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: $Revision: 4685 $

Log (CVSS: 0.0)
NVT: Fingerprint web server with favicon.ico

Summary
The remote web server contains a graphic image that is prone to information disclosure.

Vulnerability Detection Result
The following apps/services were identified:
"Joomla!" fingerprinted by the file: "http://192.168.27.45http://bt.example.net/
↪webexploitation_package_02/joomla107/images/favicon.ico"
"Joomla!" fingerprinted by the file: "http://192.168.27.45http://bt.example.net/
↪webexploitation_package_02/joomla107/images/favicon.ico"
"Joomla!" fingerprinted by the file: "http://192.168.27.45http://bt.example.net/
↪webexploitation_package_02/joomla109/images/favicon.ico"
"phpmyadmin (2.11.8.1)" fingerprinted by the file: "http://192.168.27.45/phpmyad
↪min/favicon.ico"

Impact
The 'favicon.ico' file found on the remote web server belongs to a popular webserver/application. This may be used to fingerprint the webserver/application.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: Mitigation
Remove the 'favicon.ico' file or create a custom one for your site.

Log Method
Details:`Fingerprint web server with favicon.ico`
OID:1.3.6.1.4.1.25623.1.0.20108
Version used: `$Revision: 4988 $`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result
```
The remote web server type is :
Apache/1.3.37 (Unix) PHP/4.4.4
Solution : You can set the directive "ServerTokens Prod" to limit
the information emanating from the server in its response headers.
```

Solution
Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method
Details:`HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `$Revision: 5943 $`

Log (CVSS: 0.0)
NVT: joomla Version Detection

Summary
Detection of nstalled version of joomla
This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.

Vulnerability Detection Result
```
Detected Joomla
Version:  unknown
Location: /webexploitation_package_02/joomla107
CPE:      cpe:/a:joomla:joomla
```

... continues on next page ...

... continued from previous page ...

Log Method
Details:joomla Version Detection
OID:1.3.6.1.4.1.25623.1.0.100330
Version used: $Revision: 5380 $

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

Summary
This plugin uses nikto(1) to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.

Vulnerability Detection Result

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.27.45
+ Target Hostname:    192.168.27.45
+ Target Port:        80
+ Start Time:         2017-05-26 13:41:40 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/1.3.37 (Unix) PHP/4.4.4
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
↪gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
↪to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/1.3.37 appears to be outdated (current is at least Apache/2.4.12). Apac
↪he 2.0.65 (final release) and 2.2.29 are also current.
+ PHP/4.4.4 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5
↪.4.41 are also current.
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
↪ST
+ OSVDB-3268: /./: Directory indexing found.
+ OSVDB-3268: /?mod=node&nid=some_thing&op=view: Directory indexing found.
+ OSVDB-3268: /?mod=some_thing&op=browse: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by de
↪fault if there is no index page.
+ OSVDB-3268: /?Open: Directory indexing found.
+ OSVDB-3268: /?OpenServer: Directory indexing found.
+ OSVDB-3268: /%2e/: Directory indexing found.
```

... continues on next page ...

... continued from previous page ...

```
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to
↪ v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: /?mod=<script>alert(document.cookie)</script>&op=browse: Directory
↪ indexing found.
+ OSVDB-3268: /?sql_debug=1: Directory indexing found.
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-3268: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: Directory indexing fou
↪nd.
+ OSVDB-3268: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: Directory indexing fou
↪nd.
+ OSVDB-3268: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: Directory indexing fou
↪nd.
+ OSVDB-3268: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: Directory indexing fou
↪nd.
+ OSVDB-3268: /?PageServices: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings thro
↪ugh Web Publisher by forcing the server to show all files via 'open directory
↪browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cven
↪ame.cgi?name=CVE-1999-0269.
+ OSVDB-3268: /?wp-cs-dump: Directory indexing found.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings throug
↪h Web Publisher by forcing the server to show all files via 'open directory br
↪owsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvenam
↪e.cgi?name=CVE-1999-0269.
+ Retrieved x-powered-by header: PHP/4.4.4
+ /info/: Output from the phpinfo() function was found.
+ OSVDB-3092: /info/: This might be interesting...
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databa
↪ses, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpmyadmin/ChangeLog, i
↪node: 21578, size: 10992, mtime: Sun Oct 14 23:26:43 2007
+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases,
↪ and should be protected or limited to authorized hosts.
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /manual/: Web server manual found.
+ /info.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo(
↪) was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3268: ////////////////////////////////////////////////////////////////////
↪////////////////////////////////////////////////////////////////////////////////
↪////////////////////////////////////////////////////////////////////////////////
↪//////////////////////////////////: Directory indexing found.
+ OSVDB-3288: ////////////////////////////////////////////////////////////////////
↪////////////////////////////////////////////////////////////////////////////////
↪////////////////////////////////////////////////////////////////////////////////
```

... continues on next page ...

... continued from previous page ...

```
↪//////////////////////////////: Abyss 1.03 reveals directory listing when
↪ /'s are requested.
+ OSVDB-3268: /?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3268: /?D=A: Directory indexing found.
+ OSVDB-3268: /?N=D: Directory indexing found.
+ OSVDB-3268: /?S=A: Directory indexing found.
+ OSVDB-3268: /?M=A: Directory indexing found.
+ OSVDB-3268: /?\"><script>alert('Vulnerable');</script>: Directory indexing fou
↪nd.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3268: /?_CONFIG[files][functions_page]=http://cirt.net/rfiinc.txt?: Dire
↪ctory indexing found.
+ OSVDB-3268: /?npage=-1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: Dire
↪ctory indexing found.
+ OSVDB-3268: /?npage=1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: Direc
↪tory indexing found.
+ OSVDB-3268: /?show=http://cirt.net/rfiinc.txt??: Directory indexing found.
+ /info.php?file=http://cirt.net/rfiinc.txt?: Output from the phpinfo() function
↪ was found.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSnake's list
↪ (http://ha.ckers.org/weird/rfi-locations.dat) or from http://osvdb.org/
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3268: /?-s: Directory indexing found.
+ OSVDB-3268: /?q[]=x: Directory indexing found.
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL d
↪atabases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /?sc_mode=edit: Directory indexing found.
+ OSVDB-3268: /?xmlcontrol=body%20onload=alert(123): Directory indexing found.
+ OSVDB-3268: /?admin: Directory indexing found.
+ 7534 requests: 0 error(s) and 63 item(s) reported on remote host
+ End Time:           2017-05-26 13:42:02 (GMT0) (22 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Log Method
Details:Nikto (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: $Revision: 4685 $

Log (CVSS: 0.0)
NVT: PHP Version Detection (Remote)

Summary
Detection of installed version of PHP. This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Detected PHP
Version:  4.4.4
Location: tcp/80
CPE:      cpe:/a:php:php:4.4.4
Concluded from version/product identification result:
Server: Apache/1.3.37 (Unix) PHP/4.4.4
```

Log Method
Details:PHP Version Detection (Remote)
OID:1.3.6.1.4.1.25623.1.0.800109
Version used: $Revision: 4724 $

Log (CVSS: 0.0)
NVT: PHP-Nuke Version Detection

Summary
This script detects the installed PHP-Nuke version and sets the result in KB.

Vulnerability Detection Result

```
Detected PHP-Nuke
Version:  unknown
Location: /webexploitation_package_02/phpnuke7.4
CPE:      cpe:/a:phpnuke:php-nuke
```

Log Method
Details:PHP-Nuke Version Detection
OID:1.3.6.1.4.1.25623.1.0.900338
Version used: $Revision: 5744 $

Log (CVSS: 0.0)
NVT: PHP-Nuke Version Detection

Summary
This script detects the installed PHP-Nuke version and sets the result in KB.

Vulnerability Detection Result

```
Detected PHP-Nuke
Version:  unknown
Location: /webexploitation_package_02/phpnuke7.8
CPE:      cpe:/a:phpnuke:php-nuke
```

Log Method
Details:PHP-Nuke Version Detection
OID:1.3.6.1.4.1.25623.1.0.900338
Version used: $Revision: 5744 $

Log (CVSS: 0.0)
NVT: phpBB Forum Detection

Summary
This host is running phpBB a widely installed Open Source forum solution.

Vulnerability Detection Result
```
Detected phpBB
Version:  2.0.12
Location: /webexploitation_package_02/phpBB2_2_0_12
CPE:      cpe:/a:phpbb:phpbb:2.0.12
Concluded from version/product identification result:
phpBB-2.0.11_to_2.0.12.patch
Concluded from version/product identification location:
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_12/docs/INSTALL.html
```

Log Method
Details:`phpBB Forum Detection`
OID:1.3.6.1.4.1.25623.1.0.100033
Version used: `$Revision: 4588 $`

References
```
Other:
  URL:http://www.phpbb.com
```

Log (CVSS: 0.0)
NVT: phpBB Forum Detection

Summary
This host is running phpBB a widely installed Open Source forum solution.

Vulnerability Detection Result
```
Detected phpBB
Version:  2.0.13
Location: /webexploitation_package_02/phpBB2_2_0_13
CPE:      cpe:/a:phpbb:phpbb:2.0.13
Concluded from version/product identification result:
phpBB-2.0.11_to_2.0.13.patch
Concluded from version/product identification location:
http://192.168.27.45/webexploitation_package_02/phpBB2_2_0_13/docs/INSTALL.html
```

Log Method
Details:`phpBB Forum Detection`
OID:1.3.6.1.4.1.25623.1.0.100033
Version used: `$Revision: 4588 $`

References

. . . continues on next page . . .

... continued from previous page ...

```
Other:
  URL:http://www.phpbb.com
```

Log (CVSS: 0.0)
NVT: phpMyAdmin Detection

Summary
Detection of phpMyAdmin.
The script sends a connection request to the server and attempts to extract the version number from the reply.

Vulnerability Detection Result

```
Detected phpMyAdmin
Version:  2.10.1
Location: /phpmyadmin
CPE:      cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Concluded from version/product identification result:
phpMyAdmin 2.10.1
```

Log Method
Details:`phpMyAdmin Detection`
OID:1.3.6.1.4.1.25623.1.0.900129
Version used: `$Revision: 3669 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
A web server is running on this port
```

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 5180 $`

Log (CVSS: 0.0)
NVT: WordPress Version Detection

Summary

... continues on next page ...

... continued from previous page ...

Detection of installed version of WordPress/WordPress-Mu.
This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.

Vulnerability Detection Result

```
Detected WordPress
Version:  1.5.1.1
Location: /webexploitation_package_02/wordpress
CPE:      cpe:/a:wordpress:wordpress:1.5.1.1
Concluded from version/product identification result:
WordPress 1.5.1.1
```

Log Method

Details:`WordPress Version Detection`
OID:1.3.6.1.4.1.25623.1.0.900182
Version used: `$Revision: 5871 $`

[return to 192.168.27.45]

2.1.23 Log 6000/tcp

Log (CVSS: 0.0)
NVT: Identify Unknown Services with nmap

Summary

This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.

Vulnerability Detection Result

```
Nmap service detection result for this port: X11
```

Log Method

Details:`Identify Unknown Services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5296 $`

[return to 192.168.27.45]

2.1.24 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary

... continues on next page ...

... continued from previous page ...

This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result

192.168.27.45|cpe:/a:adobe:acrobat_reader:7.0.5
192.168.27.45|cpe:/a:adobe:flash_player:7.0.63.0
192.168.27.45|cpe:/a:adobe:flash_player:9.0.31.0
192.168.27.45|cpe:/a:apache:http_server:1.3.37
192.168.27.45|cpe:/a:apple:cups:1.1
192.168.27.45|cpe:/a:foolabs:xpdf:3.01
192.168.27.45|cpe:/a:freetype:freetype:2.1.10
192.168.27.45|cpe:/a:freetype:freetype:2.2.1
192.168.27.45|cpe:/a:fwbuilder:firewall_builder:.
192.168.27.45|cpe:/a:fwbuilder:firewall_builder:1
192.168.27.45|cpe:/a:gnu:gzip:1.3.5
192.168.27.45|cpe:/a:imagemagick:imagemagick:6.2.9
192.168.27.45|cpe:/a:joomla:joomla
192.168.27.45|cpe:/a:kde:konqueror:3.5.3
192.168.27.45|cpe:/a:libgd:gd_graphics_library:5.9:7
192.168.27.45|cpe:/a:mozilla:firefox:2.0.0.4
192.168.27.45|cpe:/a:mutt:mutt:1.4.2.2
192.168.27.45|cpe:/a:openbsd:openssh:4.4
192.168.27.45|cpe:/a:openssl:openssl:0.9.8d
192.168.27.45|cpe:/a:oracle:mysql
192.168.27.45|cpe:/a:pango:pango:...
192.168.27.45|cpe:/a:pango:pango:5.97
192.168.27.45|cpe:/a:php:php:4.4.4
192.168.27.45|cpe:/a:phpbb:phpbb:2.0.12
192.168.27.45|cpe:/a:phpbb:phpbb:2.0.13
192.168.27.45|cpe:/a:phpmyadmin:phpmyadmin:2.10.1
192.168.27.45|cpe:/a:phpnuke:php-nuke
192.168.27.45|cpe:/a:postgresql:postgresql:8.1.4
192.168.27.45|cpe:/a:proftpd:proftpd:1.3.0
192.168.27.45|cpe:/a:qemu:qemu:0.9.0
192.168.27.45|cpe:/a:rahul:dtorrent:2
192.168.27.45|cpe:/a:ruby-lang:ruby:1.8.4
192.168.27.45|cpe:/a:rubyonrails:ruby_on_rails:1.2.2
192.168.27.45|cpe:/a:samba:samba:3.0.14
192.168.27.45|cpe:/a:snort:snort:2.6.1.2.34
192.168.27.45|cpe:/a:subversion:subversion:1
192.168.27.45|cpe:/a:subversion:subversion:5.97
192.168.27.45|cpe:/a:sun:jre:1.5.0_06
192.168.27.45|cpe:/a:tor:tor:0.1.1.26.
192.168.27.45|cpe:/a:videolan:vlc_media_player:0.8.4a:a
192.168.27.45|cpe:/a:webdav:neon:0.25.5
192.168.27.45|cpe:/a:wordpress:wordpress:1.5.1.1

... continues on next page ...

... continued from previous page ...

192.168.27.45|cpe:/a:x.org:x11:11.0
192.168.27.45|cpe:/o:slackware:slackware_linux:11.0

Log Method
Details:CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 5458 $

[return to 192.168.27.45]
