

Scan Report

February 27, 2024

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 “MSF2”. The scan started at Tue Feb 27 20:13:16 2024 UTC and ended at Tue Feb 27 21:32:40 2024 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	10.0.2.4	2
2.1.1	High 8787/tcp	4
2.1.2	High general/tcp	5
2.1.3	High 3632/tcp	6
2.1.4	High 21/tcp	7
2.1.5	High 512/tcp	7
2.1.6	High 514/tcp	8
2.1.7	High 53/tcp	9
2.1.8	High 22/tcp	17
2.1.9	High 80/tcp	25
2.1.10	High 2121/tcp	103
2.1.11	High 513/tcp	106
2.1.12	High 3306/tcp	107
2.1.13	High 1524/tcp	113
2.1.14	High 5432/tcp	113
2.1.15	High 6200/tcp	118
2.1.16	High 445/tcp	119
2.1.17	High 5900/tcp	125

2.1.18	Medium 25/tcp	126
2.1.19	Medium general/tcp	134
2.1.20	Medium 23/tcp	135
2.1.21	Medium 21/tcp	135
2.1.22	Medium 53/tcp	139
2.1.23	Medium 22/tcp	152
2.1.24	Medium 80/tcp	162
2.1.25	Medium 2121/tcp	243
2.1.26	Medium 3306/tcp	247
2.1.27	Medium 5432/tcp	264
2.1.28	Medium 6667/tcp	281
2.1.29	Medium 445/tcp	283
2.1.30	Medium 5900/tcp	292
2.1.31	Low general/tcp	293
2.1.32	Low 53/tcp	294
2.1.33	Low 22/tcp	295
2.1.34	Low 80/tcp	300
2.1.35	Low 2121/tcp	306
2.1.36	Low 3306/tcp	308
2.1.37	Low 5432/tcp	309
2.1.38	Low 6667/tcp	311
2.1.39	Low 445/tcp	312
2.1.40	Log 8787/tcp	316
2.1.41	Log 25/tcp	316
2.1.42	Log general/tcp	325
2.1.43	Log 23/tcp	327
2.1.44	Log 1099/tcp	329
2.1.45	Log 3632/tcp	329
2.1.46	Log general/icmp	330
2.1.47	Log 21/tcp	330
2.1.48	Log general/CPE-T	332
2.1.49	Log 512/tcp	333
2.1.50	Log 111/tcp	333
2.1.51	Log 514/tcp	335
2.1.52	Log 53/tcp	335
2.1.53	Log 139/tcp	336
2.1.54	Log 22/tcp	336
2.1.55	Log 6000/tcp	339
2.1.56	Log 80/tcp	339
2.1.57	Log 2121/tcp	349

2.1.58	Log 3306/tcp	351
2.1.59	Log 1524/tcp	353
2.1.60	Log 5432/tcp	353
2.1.61	Log 6667/tcp	359
2.1.62	Log 445/tcp	361
2.1.63	Log 5900/tcp	364

Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.2.4	118	161	21	81	0
Total: 1	118	161	21	81	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 381 results selected by the filtering described above. Before filtering there were 381 results.

Host Authentications

Host	Protocol	Result	Port/User
10.0.2.4	SMB	Success	Protocol SMB, Port 445, User

Results per Host

10.0.2.4

Host scan start Tue Feb 27 20:14:59 2024 UTC

Host scan end Tue Feb 27 21:32:40 2024 UTC

Service (Port)	Threat Level
8787/tcp	High
general/tcp	High
3632/tcp	High
21/tcp	High
512/tcp	High
514/tcp	High
53/tcp	High
22/tcp	High
80/tcp	High
2121/tcp	High
513/tcp	High
3306/tcp	High
1524/tcp	High
5432/tcp	High
6200/tcp	High

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
445/tcp	High
5900/tcp	High
25/tcp	Medium
general/tcp	Medium
23/tcp	Medium
21/tcp	Medium
53/tcp	Medium
22/tcp	Medium
80/tcp	Medium
2121/tcp	Medium
3306/tcp	Medium
5432/tcp	Medium
6667/tcp	Medium
445/tcp	Medium
5900/tcp	Medium
general/tcp	Low
53/tcp	Low
22/tcp	Low
80/tcp	Low
2121/tcp	Low
3306/tcp	Low
5432/tcp	Low
6667/tcp	Low
445/tcp	Low
8787/tcp	Log
25/tcp	Log
general/tcp	Log
23/tcp	Log
1099/tcp	Log
3632/tcp	Log
general/icmp	Log
21/tcp	Log
general/CPE-T	Log
512/tcp	Log
111/tcp	Log
514/tcp	Log
53/tcp	Log
139/tcp	Log
22/tcp	Log
6000/tcp	Log
80/tcp	Log
2121/tcp	Log
3306/tcp	Log
1524/tcp	Log

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
5432/tcp	Log
6667/tcp	Log
445/tcp	Log
5900/tcp	Log

High 8787/tcp

High (CVSS: 10.0)

NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities

Summary

Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Vulnerability Detection Result

The service is running in \$SAFE >= 1 mode. However it is still possible to run a ↵rbitrary syscall commands on the remote host. Sending an invalid syscall the s ↵ervice returned the following response:

```
Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'syscall'"0/usr/lib/
↵ruby/1.8/drb/drb.rb:1555:in 'send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in '__se
↵nd__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'perform_without_block'"3/usr/lib/
↵ruby/1.8/drb/drb.rb:1515:in 'perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in 'm
↵ain_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in 'loop'"5/usr/lib/ruby/1.8/drb/
↵drb.rb:1585:in 'main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in 'start'"5/usr
↵/lib/ruby/1.8/drb/drb.rb:1581:in 'main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:143
↵0:in 'run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in 'start'"//usr/lib/ruby/1.8/dr
↵b/drb.rb:1427:in 'run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in 'initialize'"//us
↵r/lib/ruby/1.8/drb/drb.rb:1627:in 'new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
↵'start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
↵plemented
```

Impact

By default, Distributed Ruby does not impose restrictions on allowed hosts or set the \$SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.

Solution**Solution type:** Mitigation

Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:

- Implementing taint on untrusted input
- Setting \$SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate)

... continues on next page ...

...continued from previous page ...
- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts
Vulnerability Detection Method Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests. Details: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.108010 Version used: \$Revision: 12338 \$
References BID:47071 Other: URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=22750 URL:http://www.securityfocus.com/bid/47071 URL:http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testing/ URL:http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html

[\[return to 10.0.2.4 \]](#)

High general/tcp

High (CVSS: 10.0) NVT: OS End Of Life Detection
Product detection result cpe:/o:canonical:ubuntu_linux:8.04 Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0 ↪.105937)
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 "Ubuntu" Operating System on the remote host has reached the end of life. CPE: cpe:/o:canonical:ubuntu_linux:8.04 Installed version, build or SP: 8.04 EOL date: 2013-05-09 EOL info: https://wiki.ubuntu.com/Releases
Solution Solution type: Mitigation
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Details: OS End Of Life Detection

OID:1.3.6.1.4.1.25623.1.0.103674

Version used: \$Revision: 8927 \$

Product Detection Result

Product: cpe:/o:canonical:ubuntu_linux:8.04

Method: OS Detection Consolidation and Reporting

OID: 1.3.6.1.4.1.25623.1.0.105937)

[\[return to 10.0.2.4 \]](#)**High 3632/tcp**

High (CVSS: 9.3)

NVT: DistCC Remote Code Execution Vulnerability

Summary

DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

Vulnerability Detection Result

It was possible to execute the "id" command.

Result: uid=1(daemon) gid=1(daemon)

Impact

DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.

Solution**Solution type:** VendorFix

Vendor updates are available. Please see the references for more information.

For more information about DistCC's security see the references.

Vulnerability Detection Method

Details: DistCC Remote Code Execution Vulnerability

OID:1.3.6.1.4.1.25623.1.0.103553

Version used: \$Revision: 12032 \$

References

CVE: CVE-2004-2687

Other:

URL:<https://distcc.github.io/security.html>URL:<https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:>

... continues on next page ...

...continued from previous page ...

<↪80/archives/bugtraq/2005-03/0183.html>[\[return to 10.0.2.4 \]](#)**High 21/tcp****High (CVSS: 7.5)****NVT: vsftpd Compromised Source Packages Backdoor Vulnerability****Summary**

vsftpd is prone to a backdoor vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution**Solution type:** VendorFix

The repaired package can be downloaded from the referenced link. Please validate the package with its signature.

Affected Software/OS

The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method

Details: vsftpd Compromised Source Packages Backdoor Vulnerability

OID:1.3.6.1.4.1.25623.1.0.103185

Version used: \$Revision: 12076 \$

References

BID:48539

Other:

URL:<http://www.securityfocus.com/bid/48539>

URL:<http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>

URL:<https://security.appspot.com/vsftpd.html>

[\[return to 10.0.2.4 \]](#)**High 512/tcp**

High (CVSS: 10.0) NVT: rexec Passwordless / Unencrypted Cleartext Login
Summary This remote host is running a rexec service.
Vulnerability Detection Result The rexec service is not allowing connections from this host.
Solution Solution type: Mitigation Disable the rexec service and use alternatives like SSH instead.
Vulnerability Insight rexec (Remote Process Execution) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer. The main difference is that rexec authenticates by reading the username and password *unencrypted* from the socket.
Vulnerability Detection Method Details: rexec Passwordless / Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.100111 Version used: \$Revision: 13541 \$
References Other: URL: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0618

[\[return to 10.0.2.4 \]](#)

High 514/tcp

High (CVSS: 7.5) NVT: rsh Unencrypted Cleartext Login
Summary This remote host is running a rsh service.
Vulnerability Detection Result The rsh service is misconfigured so it is allowing connections without a password or with default root:root credentials.
Solution Solution type: Mitigation Disable the rsh service and use alternatives like SSH instead.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network.
Vulnerability Detection Method Details: rsh Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.100080 Version used: \$Revision: 13010 \$
References Other: URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651

[\[return to 10.0.2.4 \]](#)

High 53/tcp

High (CVSS: 10.0) NVT: BIND End of Life Detection (Linux)
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
Summary The BIND version on the remote host has reached the end of life and should not be used anymore.
Vulnerability Detection Result The "BIND" version on the remote host has reached the end of life. CPE: cpe:/a:isc:bind:9.4.2 Installed version: 9.4.2 EOL version: 9.4 EOL date: 2009-12-31
Impact An end of life version of BIND 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 BIND version on the remote host to a still supported version.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: BIND End of Life Detection (Linux)
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.113016 Version used: \$Revision: 11935 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References Other: URL:https://www.isc.org/downloads/software-support-policy/ URL:https://www.isc.org/downloads/

High (CVSS: 7.8) NVT: ISC BIND 'buffer.c' Assertion Failure Denial of Service Vulnerability (Linux)
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
Summary The host is installed with ISC BIND and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.9.9-P3
Impact Successful exploitation will allow remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.
Solution Solution type: VendorFix Upgrade to ISC BIND version 9.9.9-P3 or 9.10.4-P3 or 9.11.0rc3 or later on Linux.
Affected Software/OS ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 on Linux.
Vulnerability Insight The flaw exists due to the 'buffer.c' script in named in ISC BIND does not properly construct responses.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host. Details: ISC BIND 'buffer.c' Assertion Failure Denial of Service Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.810263 Version used: \$Revision: 11863 \$</p>
<p>Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)</p>
<p>References CVE: CVE-2016-2776 BID:93188 Other: URL:https://kb.isc.org/article/AA-01419/0 URL:https://www.isc.org</p>

<p>High (CVSS: 7.8) NVT: ISC BIND 'buffer.c' Script Remote Denial of Service Vulnerability - Jan16</p>
<p>Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)</p>
<p>Summary The host is installed with ISC BIND and is prone to remote denial of service vulnerability.</p>
<p>Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.9.7-P3</p>
<p>Impact Successful exploitation will allow remote attackers to cause denial of service.</p>
<p>Solution Solution type: VendorFix Upgrade to ISC BIND version 9.9.7-P3 or 9.10.2-P4 or later.</p>
<p>Affected Software/OS ISC BIND versions 9.0.0 through 9.8.8 and 9.9.0 through 9.9.7-P2 and 9.10.x through 9.10.2-P3.</p>
<p>Vulnerability Insight The flaw is due to an error in 'buffer.c' script in ISC BIND.</p>
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: ISC BIND 'buffer.c' Script Remote Denial of Service Vulnerability - Jan16

OID:1.3.6.1.4.1.25623.1.0.807202

Version used: \$Revision: 11961 \$

Product Detection Result

Product: cpe:/a:isc:bind:9.4.2

Method: Determine which version of BIND name daemon is running

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

CVE: CVE-2015-5722

BID:76605

Other:

URL:<https://kb.isc.org/article/AA-01287>URL:<https://www.isc.org>

High (CVSS: 7.6)

NVT: ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability

Product detection result

cpe:/a:isc:bind:9.4.2

Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)

Summary

ISC BIND 9 is prone to a remote cache-poisoning vulnerability.

Vulnerability Detection Result

Installed version: 9.4.2

Fixed version: 9.4.3-P5

Impact

An attacker may leverage this issue to manipulate cache data, potentially facilitating man-in-the-middle, site-impersonation, or denial-of- service attacks.

Solution**Solution type:** VendorFix

Updates are available. Please see the references for details.

Affected Software/OS

Versions prior to the following are vulnerable:

... continues on next page ...

...continued from previous page ...
BIND 9.4.3-P5 BIND 9.5.2-P2 BIND 9.6.1-P3
Vulnerability Detection Method Details: ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability OID:1.3.6.1.4.1.25623.1.0.100458 Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2010-0097, CVE-2010-0290, CVE-2010-0382 BID:37865 Other: URL:http://www.securityfocus.com/bid/37865 URL:http://www.isc.org/products/BIND/ URL:http://www.kb.cert.org/vuls/id/360341 URL:https://www.isc.org/advisories/CVE-2010-0097

High (CVSS: 7.8) NVT: ISC BIND Delegation Handling Denial of Service Vulnerability
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
Summary The host is installed with ISC BIND and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: Upgrade to 9.9.6-P1
Impact Successful exploitation will allow attackers to cause denial of service to clients.
Solution Solution type: VendorFix Upgrade to ISC BIND version 9.9.6-p1 or 9.10.1-p1 or later for branches of BIND (9.9 and 9.10).
Affected Software/OS ... continues on next page ...

...continued from previous page ...
ISC BIND versions 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1
Vulnerability Insight The flaw is due to ISC BIND does not handle delegation chaining properly.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND Delegation Handling Denial of Service Vulnerability OID: 1.3.6.1.4.1.25623.1.0.806080 Version used: \$Revision: 11872 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2014-8500 Other: URL: https://kb.isc.org/article/AA-01216/0/ URL: https://www.isc.org

High (CVSS: 7.8) NVT: ISC BIND Denial of Service Vulnerability
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
Summary ISC BIND is prone to a denial of service vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.9.9-P3
Impact An remote attacker may cause a denial of service condition.
Solution Solution type: VendorFix Upgrade to 9.9.9-P3, 9.9.9-S5, 9.10.4-P3, 9.11.0rc3 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS BIND 9
Vulnerability Insight A crafted query could crash the BIND name server daemon, leading to a denial of service. All server roles (authoritative, recursive and forwarding) in default configurations are affected.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.106291 Version used: \$Revision: 12096 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2016-2776 Other: URL: https://kb.isc.org/article/AA-01419

High (CVSS: 7.8) NVT: ISC BIND Denial of Service Vulnerability - 06 - Jan16
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
Summary The host is installed with ISC BIND and is prone to remote denial of service vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.9.7-P2
Impact Successful exploitation will allow remote attackers to cause denial of service.
Solution Solution type: VendorFix Upgrade to ISC BIND version 9.9.7-P2 or 9.10.2-P3 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS ISC BIND versions 9.1.0 through 9.9.7-P1, 9.10.0 through 9.10.2-P2.
Vulnerability Insight The flaw is due to an error in handling TKEY queries can cause named to exit with a REQUIRE assertion failure.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND Denial of Service Vulnerability - 06 - Jan16 OID:1.3.6.1.4.1.25623.1.0.807200 Version used: \$Revision: 12149 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2015-5477 BID:76092 Other: URL: https://kb.isc.org/article/AA-01272 URL: https://www.isc.org

High (CVSS: 7.8) NVT: ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability - Jan16
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
Summary The host is installed with ISC BIND and is prone to remote denial of service vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.7.7
Impact Successful exploitation will allow attackers to cause denial of service.
... continues on next page ...

...continued from previous page ...
Solution Solution type: VendorFix Upgrade to ISC BIND version 9.7.7 or 9.7.6-P4 or 9.6-ESV-R8 or 9.6-ESV-R7-P4 or 9.8.4 or 9.8.3-P4 or 9.9.2 or 9.9.1-P4 later.
Affected Software/OS ISC BIND versions 9.2.x through 9.6.x, 9.4-ESV through 9.4-ESV-R5-P1, 9.6-ESV through 9.6-ESV-R7-P3, 9.7.0 through 9.7.6-P3, 9.8.0 through 9.8.3-P3, 9.9.0 through 9.9.1-P3.
Vulnerability Insight The flaw exists due to an error in DNS RDATA Handling in ISC BIND.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability - Jan16 OID:1.3.6.1.4.1.25623.1.0.807203 Version used: \$Revision: 12051 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2012-5166 BID:55852 Other: URL: https://kb.isc.org/article/AA-00801 URL: https://www.isc.org

[\[return to 10.0.2.4 \]](#)

High 22/tcp

High (CVSS: 7.5) NVT: OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability
Product detection result cpe:/a:openbsd:openssh:4.7p1 Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
Summary OpenSSH is prone to a remote memory-corruption vulnerability.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 4.7p1 Fixed version: See references
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 Solution type: VendorFix 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 Checks if a vulnerable version is present on the target host. Details: OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability OID:1.3.6.1.4.1.25623.1.0.105001 Version used: \$Revision: 12095 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 Method: SSH Server type and version OID: 1.3.6.1.4.1.25623.1.0.10267)
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:4.7p1

Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

... continues on next page ...

...continued from previous page ...
Summary This host is installed with openssh and is prone to denial of service and user enumeration vulnerabilities.
Vulnerability Detection Result Installed version: 4.7p1 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.
Solution Solution type: VendorFix Upgrade to OpenSSH version 7.3 or later.
Affected Software/OS OpenSSH versions before 7.3 on Linux
Vulnerability Insight Multiple flaws exist 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.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux) OID:1.3.6.1.4.1.25623.1.0.809154 Version used: \$Revision: 11969 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 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
... continues on next page ...

...continued from previous page ...
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:4.7p1 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: 4.7p1 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.
Solution Solution type: VendorFix Upgrade to OpenSSH 7.0 or later.
Affected Software/OS 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 Checks if a vulnerable version is present on the target host. Details: OpenSSH Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.806052 Version used: \$Revision: 11872 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 Method: SSH Server type and version OID: 1.3.6.1.4.1.25623.1.0.10267)
... continues on next page ...

...continued from previous page ...

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>URL: <http://www.openssh.com>

High (CVSS: 7.5)

NVT: OpenSSH Multiple Vulnerabilities Jan17 (Linux)

Product detection result

cpe:/a:openbsd:openssh:4.7p1

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: 4.7p1

Fixed version: 7.4

Impact

Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a serial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules.

Solution**Solution type:** VendorFix

Upgrade to OpenSSH version 7.4 or later.

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.
- NULL pointer dereference error due to an out-of-sequence NEWKEYS message.

Vulnerability Detection Method

... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host.</p> <p>Details: OpenSSH Multiple Vulnerabilities Jan17 (Linux)</p> <p>OID:1.3.6.1.4.1.25623.1.0.8103256</p> <p>Version used: \$Revision: 12467 \$</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:openbsd:openssh:4.7p1</p> <p>Method: SSH Server type and version</p> <p>OID: 1.3.6.1.4.1.25623.1.0.10267)</p>
<p>References</p> <p>CVE: CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10013, CVE-2016-10014, CVE-2016-10015, CVE-2016-10016, CVE-2016-10017, CVE-2016-10018, CVE-2016-10019, CVE-2016-10020, CVE-2016-10021, CVE-2016-10022, CVE-2016-10023, CVE-2016-10024, CVE-2016-10025, CVE-2016-10026, CVE-2016-10027, CVE-2016-10028, CVE-2016-10029, CVE-2016-10030, CVE-2016-10031, CVE-2016-10032, CVE-2016-10033, CVE-2016-10034, CVE-2016-10035, CVE-2016-10036, CVE-2016-10037, CVE-2016-10038, CVE-2016-10039, CVE-2016-10040, CVE-2016-10041, CVE-2016-10042, CVE-2016-10043, CVE-2016-10044, CVE-2016-10045, CVE-2016-10046, CVE-2016-10047, CVE-2016-10048, CVE-2016-10049, CVE-2016-10050, CVE-2016-10051, CVE-2016-10052, CVE-2016-10053, CVE-2016-10054, CVE-2016-10055, CVE-2016-10056, CVE-2016-10057, CVE-2016-10058, CVE-2016-10059, CVE-2016-10060, CVE-2016-10061, CVE-2016-10062, CVE-2016-10063, CVE-2016-10064, CVE-2016-10065, CVE-2016-10066, CVE-2016-10067, CVE-2016-10068, CVE-2016-10069, CVE-2016-10070, CVE-2016-10071, CVE-2016-10072, CVE-2016-10073, CVE-2016-10074, CVE-2016-10075, CVE-2016-10076, CVE-2016-10077, CVE-2016-10078, CVE-2016-10079, CVE-2016-10080, CVE-2016-10081, CVE-2016-10082, CVE-2016-10083, CVE-2016-10084, CVE-2016-10085, CVE-2016-10086, CVE-2016-10087, CVE-2016-10088, CVE-2016-10089, CVE-2016-10090, CVE-2016-10091, CVE-2016-10092, CVE-2016-10093, CVE-2016-10094, CVE-2016-10095, CVE-2016-10096, CVE-2016-10097, CVE-2016-10098, CVE-2016-10099, CVE-2016-10100, CVE-2016-10101, CVE-2016-10102, CVE-2016-10103, CVE-2016-10104, CVE-2016-10105, CVE-2016-10106, CVE-2016-10107, CVE-2016-10108, CVE-2016-10109, CVE-2016-10110, CVE-2016-10111, CVE-2016-10112, CVE-2016-10113, CVE-2016-10114, CVE-2016-10115, CVE-2016-10116, CVE-2016-10117, CVE-2016-10118, CVE-2016-10119, CVE-2016-10120, CVE-2016-10121, CVE-2016-10122, CVE-2016-10123, CVE-2016-10124, CVE-2016-10125, CVE-2016-10126, CVE-2016-10127, CVE-2016-10128, CVE-2016-10129, CVE-2016-10130, CVE-2016-10131, CVE-2016-10132, CVE-2016-10133, CVE-2016-10134, CVE-2016-10135, CVE-2016-10136, CVE-2016-10137, CVE-2016-10138, CVE-2016-10139, CVE-2016-10140, CVE-2016-10141, CVE-2016-10142, CVE-2016-10143, CVE-2016-10144, CVE-2016-10145, CVE-2016-10146, CVE-2016-10147, CVE-2016-10148, CVE-2016-10149, CVE-2016-10150, CVE-2016-10151, CVE-2016-10152, CVE-2016-10153, CVE-2016-10154, CVE-2016-10155, CVE-2016-10156, CVE-2016-10157, CVE-2016-10158, CVE-2016-10159, CVE-2016-10160, CVE-2016-10161, CVE-2016-10162, CVE-2016-10163, CVE-2016-10164, CVE-2016-10165, CVE-2016-10166, CVE-2016-10167, CVE-2016-10168, CVE-2016-10169, CVE-2016-10170, CVE-2016-10171, CVE-2016-10172, CVE-2016-10173, CVE-2016-10174, CVE-2016-10175, CVE-2016-10176, CVE-2016-10177, CVE-2016-10178, CVE-2016-10179, CVE-2016-10180, CVE-2016-10181, CVE-2016-10182, CVE-2016-10183, CVE-2016-10184, CVE-2016-10185, CVE-2016-10186, CVE-2016-10187, CVE-2016-10188, CVE-2016-10189, CVE-2016-10190, CVE-2016-10191, CVE-2016-10192, CVE-2016-10193, CVE-2016-10194, CVE-2016-10195, CVE-2016-10196, CVE-2016-10197, CVE-2016-10198, CVE-2016-10199, CVE-2016-10200, CVE-2016-10201, CVE-2016-10202, CVE-2016-10203, CVE-2016-10204, CVE-2016-10205, CVE-2016-10206, CVE-2016-10207, CVE-2016-10208, CVE-2016-10209, CVE-2016-10210, CVE-2016-10211, CVE-2016-10212, CVE-2016-10213, CVE-2016-10214, CVE-2016-10215, CVE-2016-10216, CVE-2016-10217, CVE-2016-10218, CVE-2016-10219, CVE-2016-10220, CVE-2016-10221, CVE-2016-10222, CVE-2016-10223, CVE-2016-10224, CVE-2016-10225, CVE-2016-10226, CVE-2016-10227, CVE-2016-10228, CVE-2016-10229, CVE-2016-10230, CVE-2016-10231, CVE-2016-10232, CVE-2016-10233, CVE-2016-10234, CVE-2016-10235, CVE-2016-10236, CVE-2016-10237, CVE-2016-10238, CVE-2016-10239, CVE-2016-10240, CVE-2016-10241, CVE-2016-10242, CVE-2016-10243, CVE-2016-10244, CVE-2016-10245, CVE-2016-10246, CVE-2016-10247, CVE-2016-10248, CVE-2016-10249, CVE-2016-10250, CVE-2016-10251, CVE-2016-10252, CVE-2016-10253, CVE-2016-10254, CVE-2016-10255, CVE-2016-10256, CVE-2016-10257, CVE-2016-10258, CVE-2016-10259, CVE-2016-10260, CVE-2016-10261, CVE-2016-10262, CVE-2016-10263, CVE-2016-10264, CVE-2016-10265, CVE-2016-10266, CVE-2016-10267, CVE-2016-10268, CVE-2016-10269, CVE-2016-10270, CVE-2016-10271, CVE-2016-10272, CVE-2016-10273, CVE-2016-10274, CVE-2016-10275, CVE-2016-10276, CVE-2016-10277, CVE-2016-10278, CVE-2016-10279, CVE-2016-10280, CVE-2016-10281, CVE-2016-10282, CVE-2016-10283, CVE-2016-10284, CVE-2016-10285, CVE-2016-10286, CVE-2016-10287, CVE-2016-10288, CVE-2016-10289, CVE-2016-10290, CVE-2016-10291, CVE-2016-10292, CVE-2016-10293, CVE-2016-10294, CVE-2016-10295, CVE-2016-10296, CVE-2016-10297, CVE-2016-10298, CVE-2016-10299, CVE-2016-10300, CVE-2016-10301, CVE-2016-10302,</p>

High (CVSS: 7.2) NVT: OpenSSH Privilege Escalation Vulnerability - May16
Product detection result cpe:/a:openbsd:openssh:4.7p1 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: 4.7p1 Fixed version: 7.2p2-3
Impact Successfully exploiting this issue will allow local users to gain privileges.
Solution Solution type: VendorFix Upgrade to OpenSSH version 7.2p2-3 or later.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
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 Checks if a vulnerable version is present on the target host. Details: OpenSSH Privilege Escalation Vulnerability - May16 OID:1.3.6.1.4.1.25623.1.0.807574 Version used: \$Revision: 11903 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 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=85bdcd7c92fe7ff133bbc4e10a65c91810f88755 URL: http://www.openssh.com
High (CVSS: 7.5) NVT: OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)
Product detection result cpe:/a:openbsd:openssh:4.7p1 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.
Vulnerability Detection Result Installed version: 4.7p1 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.
... continues on next page ...

...continued from previous page...	
Solution	
Solution type: VendorFix	
Upgrade to OpenSSH version 7.2 or later.	
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	
Checks if a vulnerable version is present on the target host.	
Details: OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)	
OID:1.3.6.1.4.1.25623.1.0.810769	
Version used: \$Revision: 11816 \$	
Product Detection Result	
Product: cpe:/a:openbsd:openssh:4.7p1	
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	
URL: http://www.openssh.com	

High (CVSS: 7.5)

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.

... continues on next page ...

...continued from previous page ...

Vulnerability Detection Result

It was possible to login with the following credentials <User>:<Password>
 user:user

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: 13568 \$

[\[return to 10.0.2.4 \]](#)

High 80/tcp

High (CVSS: 7.1)

NVT: Apache 'mod_deflate' Denial Of Service Vulnerability - July09

Product detection result

cpe:/a:apache:http_server:2.2.8

Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

Summary

This host is running Apache HTTP Server and is prone to Denial of Service vulnerability.

Vulnerability Detection Result

Installed version: 2.2.8

Fixed version: 2.2.12

Impact

Successful exploitation will allow remote attackers to cause Denial of Service to the legitimate user by CPU consumption.

Solution

Solution type: VendorFix

Update to version 2.2.12 or later.

Affected Software/OS

Apache HTTP Server version 2.2.11 and prior.

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
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: 14031 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server Detection OID: 1.3.6.1.4.1.25623.1.0.900498)
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.
Solution Solution type: VendorFix Upgrade to Apache HTTP Server version 2.2.15 or later
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.
... continues on next page ...

...continued from previous page ...
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: 14335 \$
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 URL:http://www.apache.org/

High (CVSS: 7.1) NVT: Apache 'mod_proxy_http.c' Denial Of Service Vulnerability
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
Summary This host is running Apache HTTP Server and is prone to Denial of Service vulnerability.
Vulnerability Detection Result Installed version: 2.2.8 Fixed version: 2.3.3
Impact Successful exploitation will allow remote attackers to cause Denial of Service to the legitimate user by CPU consumption.
Solution Solution type: VendorFix Update to version 2.3.3 or later.
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 ... continues on next page ...

...continued from previous page ...
Details: Apache 'mod_proxy_http.c' Denial Of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.800827 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server Detection OID: 1.3.6.1.4.1.25623.1.0.900498)
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=790587&pathrev=790587

High (CVSS: 7.5) NVT: Apache HTTP Server Multiple Vulnerabilities June17 (Linux)
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
Summary This host is running Apache HTTP Server and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 2.2.8 Fixed version: 2.2.33
Impact Successful exploitation will allow remote attackers to bypass authentication and perform unauthorized actions, cause a denial-of-service condition and gain access to potentially sensitive information.
Solution Solution type: VendorFix Upgrade to Apache HTTP Server 2.2.33 or 2.4.26 or later.
Affected Software/OS Apache HTTP Server 2.2.x before 2.2.33 and 2.4.x before 2.4.26 on Linux.
... continues on next page ...

...continued from previous page ...

Vulnerability Insight

Multiple flaws exists as,

- The mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
- The mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
- An use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: Apache HTTP Server Multiple Vulnerabilities June17 (Linux)

OID:1.3.6.1.4.1.25623.1.0.811214

Version used: \$Revision: 11863 \$

Product Detection Result

Product: cpe:/a:apache:http_server:2.2.8

Method: Apache Web Server Detection

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

CVE: CVE-2017-7679, CVE-2017-3169, CVE-2017-3167

BID:99135, 99134

Other:

URL:<http://seclists.org/oss-sec/2017/q2/509>URL:http://httpd.apache.org/security/vulnerabilities_24.htmlURL:http://httpd.apache.org/security/vulnerabilities_22.htmlURL:<https://httpd.apache.org>

High (CVSS: 10.0)

NVT: Apache Multiple Security Vulnerabilities

Product detection result

cpe:/a:apache:http_server:2.2.8

Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

Summary

Apache is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 2.2.8

Fixed version: 2.2.15

Impact

... continues on next page ...

...continued from previous page ...
These issues may lead to information disclosure or other attacks.
Solution Solution type: VendorFix Upgrade to Apache 2.2.15 or Later.
Affected Software/OS Apache versions prior to 2.2.15 are affected.
Vulnerability Detection Method Details: Apache Multiple Security Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100514 Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server Detection OID: 1.3.6.1.4.1.25623.1.0.900498)
References CVE: CVE-2010-0425, CVE-2010-0434, CVE-2010-0408, CVE-2007-6750 BID:38494, 38491 Other: URL:http://www.securityfocus.com/bid/38494 URL:http://httpd.apache.org/security/vulnerabilities_22.html URL:http://httpd.apache.org/ URL:https://issues.apache.org/bugzilla/show_bug.cgi?id=48359 URL:http://svn.apache.org/viewvc?view=revision&revision=917870

High (CVSS: 10.0)
NVT: Apache Web Server End Of Life Detection (Linux)

Product detection result
cpe:/a:apache:http_server:2.2.8
Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

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 on the remote host has reached the end of life.
CPE: cpe:/a:apache:http_server:2.2.8
Installed version: 2.2.8
EOL version: 2.2

...continues on next page ...

...continued from previous page ...	
EOL date:	2017-12-31
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 Checks if a vulnerable version is present on the target host. Details: Apache Web Server End Of Life Detection (Linux) OID:1.3.6.1.4.1.25623.1.0.108085 Version used: \$Revision: 11863 \$	
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server 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://www.apache.org/dist/httpd/Announcement2.2.html URL:https://en.wikipedia.org/wiki/Apache_HTTP_Server#Versions	

High (CVSS: 9.3) NVT: PHP '_gdGetColors()' Buffer Overflow Vulnerability	
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)	
Summary The host is running PHP and is prone to Buffer Overflow vulnerability.	
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.12/5.3.1	
Impact ... continues on next page ...	

...continued from previous page ...
Successful exploitation could allow attackers to potentially compromise a vulnerable system.
Solution Solution type: VendorFix Update to version 5.2.12, 5.3.1 or later.
Affected Software/OS PHP version 5.2.x to 5.2.11 and 5.3.0 on Linux.
Vulnerability Insight The flaw is due to error in '_gdGetColors' function in gd_gd.c which fails to check certain colorsTotal structure member, which can be exploited to cause buffer overflow or buffer over-read attacks via a crafted GD file.
Vulnerability Detection Method Details: PHP '_gdGetColors()' Buffer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.801123 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2009-3546 BID:36712 Other: URL:http://secunia.com/advisories/37080/ URL:http://www.vupen.com/english/advisories/2009/2930 URL:http://marc.info/?l=oss-security&m=125562113503923&w=2
High (CVSS: 7.5) NVT: PHP 'libgd' Denial of Service Vulnerability (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4
... continues on next page ...

...continued from previous page ...	
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.	
Solution Solution type: VendorFix Update to PHP version 5.6.27 or 7.0.12.	
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 exists due to an integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'libgd' Denial of Service Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.809338 Version used: \$Revision: 11811 \$	
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)	
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 URL:http://www.php.net	
High (CVSS: 10.0) NVT: PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Linux)	
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)	
... continues on next page ...	

...continued from previous page ...
Summary This host is installed with PHP and is prone to stack buffer overflow vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later.
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 Checks if a vulnerable version is present on the target host. 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: 12149 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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

<p>High (CVSS: 7.5) NVT: PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Linux)</p>
<p>Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary This host is installed with PHP and is prone to remote code execution vulnerability.</p>
<p>Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.4.45</p>
<p>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.</p>
<p>Solution Solution type: VendorFix Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later.</p>
<p>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</p>
<p>Vulnerability Insight The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. 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: 12431 \$</p>
<p>Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References CVE: CVE-2015-6836 BID:76644 Other:</p>
<p>... continues on next page ...</p>

...continued from previous page ...

URL: <http://www.php.net/ChangeLog-5.php>
 URL: <https://bugs.php.net/bug.php?id=70388>

High (CVSS: 7.5)**NVT: PHP 'shmop_read()' Remote Integer Overflow Vulnerability****Product detection result**

cpe:/a:php:php:5.2.4

Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is prone to an integer-overflow vulnerability because it fails to ensure that integer values are not overrun.

Vulnerability Detection Result

Installed version: 5.2.4

Fixed version: 5.3.6

Impact

Successful exploits of this vulnerability allow remote attackers to execute arbitrary code in the context of a webserver affected by the issue. Failed attempts will likely result in denial-of-service conditions.

Solution**Solution type:** VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Versions prior to PHP 5.3.6 are vulnerable.

Vulnerability Detection Method

Details: PHP 'shmop_read()' Remote Integer Overflow Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.103113

Version used: \$Revision: 10458 \$

Product Detection Result

Product: cpe:/a:php:php:5.2.4

Method: PHP Version Detection (Remote)

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

CVE: CVE-2011-1092

BID: 46786

Other:

... continues on next page ...

...continued from previous page ...
URL: https://www.securityfocus.com/bid/46786
URL: http://comments.gmane.org/gmane.comp.security.oss.general/4436
URL: http://www.php.net/
URL: http://svn.php.net/viewvc/?view=revision&revision=309018

High (CVSS: 7.5) NVT: PHP 'SplObjectStorage' Unserializer Arbitrary Code Execution Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
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: 5.2.4 Fixed version: 5.3.3
Impact Successful exploits will compromise the application and possibly the computer.
Solution Solution type: VendorFix Updates are available. Please see the references for details.
Affected Software/OS PHP 5 through 5.3.2 are vulnerable.
Vulnerability Detection Method Details: PHP 'SplObjectStorage' Unserializer Arbitrary Code Execution Vulnerability OID: 1.3.6.1.4.1.25623.1.0.100684 Version used: \$Revision: 10459 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2010-2225 BID: 40948 Other:
... continues on next page ...

...continued from previous page ...
URL:https://www.securityfocus.com/bid/40948 URL:https://bugzilla.redhat.com/show_bug.cgi?id=605641 URL:http://www.php.net
High (CVSS: 7.5) NVT: PHP 'sqlite_single_query()' and 'sqlite_array_query()' Arbitrary Code Execution Vulnerabilities
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities that may allow attackers to execute arbitrary code.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.3.3/5.2.14
Impact Attackers can exploit these issues to run arbitrary code within the context of the PHP process. This may allow them to bypass intended security restrictions or gain elevated privileges.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS PHP 5.3.0 through 5.3.2, PHP 5.2.0 through 5.2.13 are vulnerable
Vulnerability Detection Method Details: PHP 'sqlite_single_query()' and 'sqlite_array_query()' Arbitrary Code Execution. ↪.. OID:1.3.6.1.4.1.25623.1.0.100631 Version used: \$Revision: 10459 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2010-1868 BID:40013 ... continues on next page ...

...continued from previous page ...
Other: URL:http://www.securityfocus.com/bid/40013 URL:http://php-security.org/2010/05/07/mops-2010-012-php-sqlite_single_query- ↪uninitialized-memory-usage-vulnerability/index.html URL:http://php-security.org/2010/05/07/mops-2010-013-php-sqlite_array_query-u ↪ninitialized-memory-usage-vulnerability/index.html URL:http://www.php.net URL:http://php-security.org/2010/05/07/mops-submission-03-sqlite_single_query ↪-sqlite_array_query-uninitialized-memory-usage/index.html

High (CVSS: 7.5) NVT: PHP 'substr_replace()' Use After Free Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is running PHP and is prone to Use After Free vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.3.7 or later.
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: 11997 \$
Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 URL: http://www.php.net/downloads.php

High (CVSS: 10.0) NVT: PHP 'type confusion' Denial of Service Vulnerability (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.7
Impact Successfully exploiting this issue allow remote attackers to cause a denial of service.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.7 or later.
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 Checks if a vulnerable version is present on the target host. Details: PHP 'type confusion' Denial of Service Vulnerability (Linux) OID: 1.3.6.1.4.1.25623.1.0.808673
... continues on next page ...

...continued from previous page ...
Version used: \$Revision: 14181 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.26
Impact Successfully exploiting this issue allow remote attackers to cause a denial of service.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.26, or later.
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 Checks if a vulnerable version is present on the target host. Details: PHP 'var_unserializer' Denial of Service Vulnerability (Linux)
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.809321 Version used: \$Revision: 11938 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2016-7411 BID:93009 Other: URL:http://www.php.net/ChangeLog-5.php

High (CVSS: 10.0) NVT: PHP < 5.2.12 Multiple Vulnerabilities
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to a cross-site scripting vulnerability and to a code execution vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.12
Impact Attackers can exploit the code execution vulnerability to execute arbitrary code within the context of the PHP process. This may allow them to bypass intended security restrictions or gain elevated privileges. An attacker may leverage the cross-site scripting vulnerability 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 Versions prior to PHP 5.2.12 are vulnerable.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
Details: PHP < 5.2.12 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100409 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2009-4143, CVE-2009-4142 BID:37390, 37389 Other: URL:http://www.securityfocus.com/bid/37390 URL:http://www.securityfocus.com/bid/37389 URL:http://www.php.net/ChangeLog-5.php#5.2.12 URL:http://www.php.net/releases/5_2_12.php URL:http://www.php.net URL:http://www.suspekt.org/downloads/POC2009-ShockingNewsInPHPExploitation.pdf ↪f URL:http://www.blackhat.com/presentations/bh-usa-09/ESSER/BHUSA09-Esser-PostE ↪xploitationPHP-PAPER.pdf URL:http://d.hatena.ne.jp/t_komura/20091004/1254665511 URL:http://bugs.php.net/bug.php?id=49785

High (CVSS: 7.5) NVT: PHP < 5.2.13 Multiple Vulnerabilities
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The remote web server has installed a PHP Version which is prone to Multiple Vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.13
Solution Solution type: VendorFix Updates are available. Please see the references for details.
Affected Software/OS
... continues on next page ...

...continued from previous page ...
PHP versions prior to 5.2.13 are affected.
Vulnerability Insight Multiple vulnerabilities exist due to: <ol style="list-style-type: none"> 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: 13960 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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/session ↪n.c?r1=293036&r2=294272 URL:http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/session/session ↪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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to arbitrary code execution vulnerability
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.5.27
Impact Successfully exploiting this issue allow remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.27, or 5.6.11, or later.
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 Checks if a vulnerable version is present on the target host. Details: PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808671 Version used: \$Revision: 11903 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
... continues on next page ...

...continued from previous page ...
Summary This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.32, or 5.6.18, or 7.0.3, or later.
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 Checks if a vulnerable version is present on the target host. 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: 12149 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4
... continues on next page ...

...continued from previous page ...
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.28, or 5.6.12, or later.
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 Checks if a vulnerable version is present on the target host. Details: PHP Denial of Service Vulnerability - 01 - Jul16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808613 Version used: \$Revision: 14181 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109
References CVE: CVE-2015-8878 BID:90837 Other: URL:http://www.php.net/ChangeLog-5.php
High (CVSS: 7.8) NVT: PHP Denial of Service Vulnerability Jul17 (Linux)
... continues on next page ...

...continued from previous page ...
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.31
Impact Successfully exploiting this issue allow an attacker to cause a CPU consumption denial of service attack.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.31, 7.0.17, 7.1.3 or later.
Affected Software/OS PHP versions before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3
Vulnerability Insight The flaw exists due to improper handling of long form variables in main/php_variables.c script.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Denial of Service Vulnerability Jul17 (Linux) OID:1.3.6.1.4.1.25623.1.0.811487 Version used: \$Revision: 11874 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2017-11142 Other: URL: http://www.php.net/ChangeLog-5.php URL: http://www.php.net/ChangeLog-7.php
High (CVSS: 7.5) NVT: PHP Directory Traversal Vulnerability - Jul16 (Linux)
... continues on next page ...

...continued from previous page ...
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to Directory traversal vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.4.45, or 5.5.29, or 5.6.13, or later.
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 <ul style="list-style-type: none"> - 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 Checks if a vulnerable version is present on the target host. Details: PHP Directory Traversal Vulnerability - Jul16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808617 Version used: \$Revision: 14181 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2014-9767, CVE-2015-6834, CVE-2015-6835, CVE-2015-6837, CVE-2015-6838 BID:76652, 76649, 76733, 76738
... continues on next page ...

...continued from previous page ...	
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)	
Summary The PHP version on the remote host has reached the end of life and should not be used anymore.	
Vulnerability Detection Result The "PHP" version on the remote host has reached the end of life. CPE: cpe:/a:php:php:5.2.4 Installed version: 5.2.4 EOL version: 5.2 EOL date: 2011-01-06	
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.	
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 Checks if a vulnerable version is present on the target host. Details: PHP End Of Life Detection (Linux) OID:1.3.6.1.4.1.25623.1.0.105889 Version used: \$Revision: 12149 \$	
... continues on next page ...	

...continued from previous page ...
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References Other: URL: https://secure.php.net/supported-versions.php URL: https://secure.php.net/eol.php

High (CVSS: 10.0) NVT: PHP Heap-based buffer overflow in 'mbstring' extension
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The host is running PHP and is prone to Buffer Overflow vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.7
Impact Successful exploitation could allow attackers to execute arbitrary code via a crafted string containing an HTML entity.
Solution Solution type: VendorFix Upgrade to version 5.2.7 or later.
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: 14010 \$
... continues on next page ...

...continued from previous page ...
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 Interruptions and Calltime Arbitrary Code Execution Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
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: 5.2.4 Fixed version: N/A
Impact Successful exploits will compromise the application and possibly the computer.
Solution Solution type: WillNotFix No known solution was made available for at least one year since the 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: PHP Interruptions and Calltime Arbitrary Code Execution Vulnerability OID: 1.3.6.1.4.1.25623.1.0.100252 Version used: \$Revision: 10459 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote)
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.800109)
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 Multiple Buffer Overflow Vulnerabilities
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple buffer-overflow vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.8
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: 13960 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote)
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.800109)
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 Buffer Overflow Vulnerabilities - Jan15
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service and arbitrary code execution vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.7
Impact Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code.
Solution Solution type: VendorFix Upgrade to PHP version 5.2.7 or later.
Affected Software/OS PHP versions 5.2.x before 5.2.7
Vulnerability Insight The multiple flaws are due to - Improper validation of user supplied input passed to date_from_ISO8601() function in xmlrpc.c - including a timezone field in a date, leading to improper XML-RPC encoding.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host.</p> <p>Details: PHP Multiple Buffer Overflow Vulnerabilities - Jan15</p> <p>OID:1.3.6.1.4.1.25623.1.0.805410</p> <p>Version used: \$Revision: 11872 \$</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:php:php:5.2.4</p> <p>Method: PHP Version Detection (Remote)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References</p> <p>CVE: CVE-2014-8626</p> <p>BID:70928</p> <p>Other:</p> <p>URL:https://bugs.php.net/bug.php?id=45226</p> <p>URL:http://openwall.com/lists/oss-security/2014/11/06/3</p>

<p>High (CVSS: 7.5)</p> <p>NVT: PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Linux)</p>
<p>Product detection result</p> <p>cpe:/a:php:php:5.2.4</p> <p>Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary</p> <p>This host is installed with PHP and is prone to multiple denial of service vulnerabilities.</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.2.4</p> <p>Fixed version: 5.6.30</p>
<p>Impact</p> <p>Successfully exploiting this issue allow remote attackers to cause a denial of service (memory consumption or application crash).</p>
<p>Solution</p> <p>Solution type: VendorFix</p> <p>Upgrade to PHP version 5.6.30, 7.0.15 or later.</p>
<p>Affected Software/OS</p> <p>PHP versions before 5.6.30 and 7.0.x before 7.0.15</p>
<p>Vulnerability Insight</p> <p>Multiple flaws are due to</p> <p>... continues on next page ...</p>

...continued from previous page ...
<ul style="list-style-type: none"> - A integer overflow in the <code>phar_parse_pharfile</code> function in <code>ext/phar/phar.c</code> via a truncated manifest entry in a PHAR archive. - A off-by-one error in the <code>phar_parse_pharfile</code> function in <code>ext/phar/phar.c</code> via a crafted PHAR archive with an alias mismatch.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Multiple Denial of Service Vulnerabilities - 02 - Jan17 (Linux) OID:1.3.6.1.4.1.25623.1.0.108054 Version used: \$Revision: 11835 \$
Product Detection Result Product: <code>cpe:/a:php:php:5.2.4</code> Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 URL: http://www.php.net

High (CVSS: 7.5) NVT: PHP Multiple Double Free Vulnerabilities - Jan15
Product detection result <code>cpe:/a:php:php:5.2.4</code> Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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.
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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Double Free Vulnerabilities - Jan15 OID:1.3.6.1.4.1.25623.1.0.805412 Version used: \$Revision: 11872 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.5.33
Impact ... continues on next page ...

...continued from previous page ...
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).
Solution Solution type: VendorFix Upgrade to PHP version 5.5.33 or 5.6.19 or later.
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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 01 - Apr16 (Linux) OID:1.3.6.1.4.1.25623.1.0.807807 Version used: \$Revision: 12431 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 URL:http://www.php.net
High (CVSS: 7.5) NVT: PHP Multiple Vulnerabilities - 01 - Aug16 (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
... continues on next page ...

...continued from previous page...	
Vulnerability Detection Result Installed version: 5.2.4 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.	
Solution Solution type: VendorFix Upgrade to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later.	
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, <ul style="list-style-type: none"> - 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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 01 - Aug16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808788 Version used: \$Revision: 12431 \$	
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)	
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	

<p>High (CVSS: 7.5) NVT: PHP Multiple Vulnerabilities - 01 - Jul16 (Linux)</p>
<p>Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary This host is installed with PHP and is prone to multiple vulnerabilities.</p>
<p>Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.5.34</p>
<p>Impact Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.</p>
<p>Solution Solution type: VendorFix Upgrade to PHP version 5.5.34, or 5.6.20, or 7.0.5, or later.</p>
<p>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</p>
<p>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.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 01 - Jul16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808199 Version used: \$Revision: 12051 \$</p>
<p>Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>... continues on next page ...</p>

...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:5.2.4

Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

This host is installed with PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 5.2.4

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.

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later.

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

Checks if a vulnerable version is present on the target host.

Details: PHP Multiple Vulnerabilities - 01 - Mar16 (Linux)

OID: 1.3.6.1.4.1.25623.1.0.807503

Version used: \$Revision: 12149 \$

Product Detection Result

... continues on next page ...

...continued from previous page ...
Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 URL: http://www.php.net

High (CVSS: 7.5) NVT: PHP Multiple Vulnerabilities - 02 - Aug16 (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.37, or 5.6.23, or later.
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.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 02 - Aug16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808790 Version used: \$Revision: 14181 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.5
Impact Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.5 or later.
Affected Software/OS PHP versions before 5.6.5
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 02 - Jan15 OID:1.3.6.1.4.1.25623.1.0.805413 Version used: \$Revision: 11872 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.25, or 7.0.10, or later.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
PHP versions prior to 5.6.25 and 7.x before 7.0.10 on Linux
Vulnerability Insight Multiple flaws are due to <ul style="list-style-type: none"> - 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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 02 - Sep16 (Linux) OID:1.3.6.1.4.1.25623.1.0.809319 Version used: \$Revision: 11961 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
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: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.36, or 5.6.22, or later.
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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 03 - Aug16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808792 Version used: \$Revision: 12313 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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
... continues on next page ...

...continued from previous page ...
cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later.
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 sprintf 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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 03 - Jul16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808603 Version used: \$Revision: 11961 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote)
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.25, or 7.0.10, or later.
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, <ul style="list-style-type: none"> - 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.
... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - 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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 03 - Sep16 (Linux) OID:1.3.6.1.4.1.25623.1.0.809317 Version used: \$Revision: 11938 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later.
... continues on next page ...

...continued from previous page ...
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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 04 - Aug16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808794 Version used: \$Revision: 11961 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.4.44
Impact ... continues on next page ...

...continued from previous page ...
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.
Solution Solution type: VendorFix Upgrade to PHP version 5.4.44, or 5.5.28, or 5.6.12, or later.
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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 04 - Jul16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808604 Version used: \$Revision: 12313 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
... continues on next page ...

...continued from previous page ...	
Vulnerability Detection Result Installed version: 5.2.4 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.	
Solution Solution type: VendorFix Upgrade to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later.	
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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 05 - Aug16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808675 Version used: \$Revision: 12313 \$	
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)	
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)	
... 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: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.38, or 5.6.24, or 7.0.9, or later.
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 <ul style="list-style-type: none"> - 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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - 05 - Jul16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808634 Version used: \$Revision: 11938 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References ... continues on next page ...

...continued from previous page ...
<p>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</p> <p>BID: 92111, 92074, 92097, 92073, 92078, 92115, 92094, 92095, 92099</p> <p>Other:</p> <p>URL: http://php.net/ChangeLog-5.php</p> <p>URL: http://php.net/ChangeLog-7.php</p> <p>URL: http://openwall.com/lists/oss-security/2016/07/24/2</p> <p>URL: http://www.php.net</p>

<p>High (CVSS: 10.0)</p> <p>NVT: PHP Multiple Vulnerabilities - Aug08</p>
<p>Product detection result</p> <p>cpe:/a:php:php:5.2.4</p> <p>Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary</p> <p>The host is installed with PHP, that is prone to multiple vulnerabilities.</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.2.4</p> <p>Fixed version: 5.2.6</p>
<p>Impact</p> <p>Successful exploitation could result in remote arbitrary code execution, security restrictions bypass, access to restricted files, denial of service.</p>
<p>Solution</p> <p>Solution type: VendorFix</p> <p>Upgrade to PHP version 5.2.6 or later.</p>
<p>Affected Software/OS</p> <p>PHP version prior to 5.2.6</p>
<p>Vulnerability Insight</p> <p>The flaws are caused by,</p> <ul style="list-style-type: none"> - 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).
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Details: PHP Multiple Vulnerabilities - Aug08 OID:1.3.6.1.4.1.25623.1.0.800110 Version used: \$Revision: 14010 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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://pcrc.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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is running PHP and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.11
Impact Successful exploitation could allow local attackers to bypass certain security restrictions and cause denial of service.
Solution Solution type: VendorFix Upgrade to version 5.3.1 or later.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
PHP version 5.2.10 and prior. PHP version 5.3.x before 5.3.1
Vulnerability Insight Multiple flaws are due to: <ul style="list-style-type: none"> - 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 Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - Dec09 OID:1.3.6.1.4.1.25623.1.0.801060 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2009-4018, CVE-2009-2626 BID:37138, 36009 Other: <ul style="list-style-type: none"> 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: 8.5) NVT: PHP Multiple Vulnerabilities - Dec18 (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple security vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.39 Installation
... continues on next page ...

...continued from previous page...	
path / port:	80/tcp
Impact Successful exploitation will allow remote attackers to execute remote code on the affected application/system and/or cause a denial of service.	
Solution Solution type: VendorFix Update to version 5.6.39, 7.0.33, 7.1.25, 7.2.13, 7.3.0 or later.	
Affected Software/OS PHP versions 5.x before 5.6.39, 7.0.x before 7.0.33, 7.1.x before 7.1.25 and 7.2.x before 7.2.13.	
Vulnerability Insight The flaws exist due to, - the imap_open functions which allows to run arbitrary shell commands via mailbox parameter. - a Heap Buffer Overflow (READ: 4) in phar_parse_pharfile. - ext/standard/var_unserializer.c allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - Dec18 (Linux) OID:1.3.6.1.4.1.25623.1.0.108507 Version used: 2019-03-29T15:39:23+0000	
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References CVE: CVE-2018-19518, CVE-2018-20783, CVE-2018-19396 BID:106018 Other: URL: https://bugs.php.net/bug.php?id=76428 URL: https://bugs.php.net/bug.php?id=77153 URL: https://bugs.php.net/bug.php?id=77160 URL: https://bugs.php.net/bug.php?id=77143 URL: http://www.securityfocus.com/bid/106018 URL: https://github.com/Bo0oM/PHP_imap_open_exploit/blob/master/exploit.php URL: https://www.exploit-db.com/exploits/45914/ URL: https://www.openwall.com/lists/oss-security/2018/11/22/3	

High (CVSS: 7.5) NVT: PHP Multiple Vulnerabilities - Feb19 (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.40 Installation path / port: 80/tcp
Solution Solution type: VendorFix Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later.
Affected Software/OS PHP versions before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14 and 7.3.x before 7.3.1.
Vulnerability Insight PHP is prone to multiple vulnerabilities: - Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c. (CVE-2019-9020) - A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name. (CVE-2019-9021) - A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. (CVE-2019-9023) - xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas (CVE-2019-9024)
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - Feb19 (Linux) OID:1.3.6.1.4.1.25623.1.0.142048 Version used: \$Revision: 13857 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
... continues on next page ...

...continued from previous page ...

References

CVE: CVE-2019-9020, CVE-2019-9021, CVE-2019-9023, CVE-2019-9024

Other:

URL:https://bugs.php.net/bug.php?id=77242
 URL:https://bugs.php.net/bug.php?id=77249
 URL:https://bugs.php.net/bug.php?id=77247
 URL:https://bugs.php.net/bug.php?id=77370
 URL:https://bugs.php.net/bug.php?id=77371
 URL:https://bugs.php.net/bug.php?id=77381
 URL:https://bugs.php.net/bug.php?id=77382
 URL:https://bugs.php.net/bug.php?id=77385
 URL:https://bugs.php.net/bug.php?id=77394
 URL:https://bugs.php.net/bug.php?id=77418
 URL:https://bugs.php.net/bug.php?id=77380

High (CVSS: 7.5)

NVT: PHP Multiple Vulnerabilities - Sep09

Product detection result

cpe:/a:php:php:5.2.4

Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

This host is running PHP and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 5.2.4

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.

Solution**Solution type:** VendorFix

Upgrade to version 5.2.11 or later.

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.

... continues on next page ...

...continued from previous page ...
- An unspecified error exists related to the sanity check for the color index in the 'imagecolor-transparent' function.
Vulnerability Detection Method Details: PHP Multiple Vulnerabilities - Sep09 OID:1.3.6.1.4.1.25623.1.0.900871 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4

Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

This host is installed with PHP and is prone to denial of service vulnerability.

Vulnerability Detection Result

Installed version: 5.2.4

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 .

Solution

Solution type: VendorFix

Upgrade to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

... continues on next page ...

...continued from previous page ...
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 Checks if a vulnerable version is present on the target host. Details: PHP Out of Bounds Read Multiple Vulnerabilities - Jan15 OID:1.3.6.1.4.1.25623.1.0.805414 Version used: \$Revision: 11872 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to remote code execution vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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).
Solution Solution type: VendorFix
... continues on next page ...

...continued from previous page ...
Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later.
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 Checks if a vulnerable version is present on the target host. 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: 11865 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 URL:http://www.php.net

High (CVSS: 7.5) NVT: PHP Security Bypass and File Writing Vulnerability - Dec08
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The host is running PHP and is prone to Security Bypass and File Writing vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.7
Impact ... continues on next page ...

...continued from previous page ...
Successful exploitation could allow remote attackers to write arbitrary file, bypass security restrictions and cause directory traversal attacks.
Solution Solution type: VendorFix Upgrade to version 5.2.7 or later.
Affected Software/OS PHP versions prior to 5.2.7.
Vulnerability Insight The flaw is due to, <ul style="list-style-type: none"> - An error in initialization of 'page_uid' and 'page_gid' global variables for use by the SAPI 'php_getuid' function, which bypass the safe_mode restrictions. - When 'safe_mode' is enabled through a 'php_admin_flag' setting in 'httpd.conf' file, which does not enforce the 'error_log', 'safe_mode' restrictions. - In 'ZipArchive::extractTo' function which allows attacker to write files via a ZIP file.
Vulnerability Detection Method Details: PHP Security Bypass and File Writing Vulnerability - Dec08 OID:1.3.6.1.4.1.25623.1.0.900184 Version used: \$Revision: 14010 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2008-5624, CVE-2008-5625, CVE-2008-5658 BID:32383, 32625, 32688 Other: URL: http://www.php.net/ChangeLog-5.php#5.2.7 URL: http://www.php.net/archive/2008.php#id2008-12-07-1 URL: http://www.securityfocus.com/archive/1/archive/1/498985/100/0/threaded

High (CVSS: 7.5)

NVT: PHP Stack Buffer Overflow Vulnerability Mar18 (Linux)

Product detection result

cpe:/a:php:php:5.2.4

Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

... continues on next page ...

...continued from previous page ...
The host is installed with php and is prone to stack buffer overflow vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.34 Installation path / port: 80/tcp
Impact Successful exploitation will allow an attacker to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.
Solution Solution type: VendorFix Upgrade to version 7.2.3, 7.0.28, 5.6.34, 7.1.15 or later.
Affected Software/OS PHP versions 7.2.x prior to 7.2.3, PHP versions 7.0.x prior to 7.0.28, PHP versions 5.0.x prior to 5.6.34 and PHP versions 7.1.x prior to 7.1.15 on Linux.
Vulnerability Insight The flaw exists because php fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Stack Buffer Overflow Vulnerability Mar18 (Linux) OID:1.3.6.1.4.1.25623.1.0.812821 Version used: \$Revision: 12391 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2018-7584 BID:103204 Other: URL:http://php.net/ChangeLog-7.php URL:https://bugs.php.net/bug.php?id=75981 URL:http://www.php.net

High (CVSS: 7.5) NVT: PHP Version < 5.2.11 Multiple Vulnerabilities
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP version smaller than 5.2.11 suffers from multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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: 10460 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP version smaller than 5.2.14 suffers from multiple vulnerabilities.
Vulnerability Detection Result ... continues on next page ...

...continued from previous page ...
Installed version: 5.2.4 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: 10460 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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: 9.3) NVT: PHP Version < 5.2.5 Multiple Vulnerabilities
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP version smaller than 5.2.5 suffers from multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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
... continues on next page ...

...continued from previous page ...
Version used: \$Revision: 10460 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP version smaller than 5.2.6 suffers from multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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: 10823 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2007-4850, CVE-2007-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, ... continues on next page ...

↔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:5.2.4

Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP version smaller than 5.2.7 suffers from multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 5.2.4

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: 11529 \$

Product Detection Result

Product: cpe:/a:php:php:5.2.4

Method: PHP Version Detection (Remote)

OID: 1.3.6.1.4.1.25623.1.0.800109)

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:5.2.4

Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

...continued from previous page ...
Summary PHP version smaller than 5.2.8 suffers from multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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: 10460 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP version smaller than 5.3.1 suffers from multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.3.1
Solution Solution type: VendorFix Update PHP to version 5.3.1 or later.
... continues on next page ...

...continued from previous page ...
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: 10460 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP version smaller than 5.3.3 suffers from multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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: 10460 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References
... continues on next page ...

...continued from previous page ...
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to multiple security vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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: 10459 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2009-3559, CVE-2009-4017 BID:37079 ... continues on next page ...

...continued from previous page ...
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-CGI-based setups vulnerability when parsing query string parameters from php files.
Summary PHP is prone to an information-disclosure vulnerability.
Vulnerability Detection Result Vulnerable url: http://10.0.2.4/cgi-bin/php
Impact Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.
Solution Solution type: VendorFix PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.
Vulnerability Insight When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution. An example of the -s command, allowing an attacker to view the source code of index.php is below: http://example.com/index.php?-s
Vulnerability Detection Method Details: PHP-CGI-based setups vulnerability when parsing query string parameters from ph. ↪.. OID:1.3.6.1.4.1.25623.1.0.103482 Version used: \$Revision: 13679 \$
References CVE: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335 BID:53388 Other:
... continues on next page ...

...continued from previous page ...
URL: http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-risks-Update-1567532.html
URL: http://www.kb.cert.org/vuls/id/520827
URL: http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
URL: https://bugs.php.net/bug.php?id=61910
URL: http://www.php.net/manual/en/security.cgi-bin.php
URL: http://www.securityfocus.com/bid/53388

High (CVSS: 7.5) NVT: <code>phpinfo()</code> output Reporting
Summary Many PHP installation tutorials instruct the user to create a file called <code>phpinfo.php</code> or similar containing the <code>phpinfo()</code> statement. Such a file is often left back in the webserver directory.
Vulnerability Detection Result The following files are calling the function <code>phpinfo()</code> which disclose potentially sensitive information: http://10.0.2.4/mutillidae/phpinfo.php http://10.0.2.4/phpinfo.php
Impact Some of the information that can be gathered from this file includes: The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.
Solution Solution type: Workaround Delete the listed files or restrict access to them.
Vulnerability Detection Method Details: <code>phpinfo()</code> output Reporting OID: 1.3.6.1.4.1.25623.1.0.11229 Version used: \$Revision: 11992 \$

High (CVSS: 7.5) NVT: <code>phpMyAdmin</code> 'CVE-2009-1285' Configuration File PHP Code Injection Vulnerability
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by <code>phpMyAdmin</code> Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary ... continues on next page ...

...continued from previous page ...
According to its version number, the remote version of phpMyAdmin is prone to a remote PHP code-injection vulnerability.
Vulnerability Detection Result Installed version: 3.1.1 Fixed version: See references
Impact An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system. Other attacks are also possible.
Solution Solution type: VendorFix Vendor updates are available.
Affected Software/OS phpMyAdmin 3.x versions prior to 3.1.3.2 are vulnerable.
Vulnerability Detection Method Details: phpMyAdmin 'CVE-2009-1285' Configuration File PHP Code Injection Vulnerability OID:1.3.6.1.4.1.25623.1.0.100144 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References CVE: CVE-2009-1285 BID:34526 Other: URL:http://www.securityfocus.com/bid/34526
High (CVSS: 7.5) NVT: phpMyAdmin 2.11.x < 2.11.9.4 / 3.0.x < 3.1.3 Multiple Vulnerabilities
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 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 multiple vulnerabilities.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 3.1.1 Fixed version: 2.11.9.5/3.1.3.1
Impact Successful exploitation will let the attacker cause XSS, Directory Traversal attacks or can injection malicious PHP Codes to gain sensitive information about the remote host.
Solution Solution type: VendorFix Upgrade to version 2.11.9.5 or 3.1.3.1 or later.
Affected Software/OS phpMyAdmin version 2.11.x to 2.11.9.4 and 3.0.x to 3.1.3.
Vulnerability Insight Multiple flaws are due to, - BLOB streaming feature in 'bs_disp_as_mime_type.php' causes CRLF Injection which lets the attacker inject arbitrary data in the HTTP headers through the 'c_type' and 'file_type' parameters. - XSS Vulnerability in 'display_export.lib.php' as its not sanitizing the 'pma_db_filename_template' parameter. - Static code injection vulnerability in 'setup.php' which can be used to inject PHP Codes. - Filename 'bs_disp_as_mime_type.php' which is not sanitizing user supplied inputs in the filename variable which causes directory traversal attacks.
Vulnerability Detection Method Details: phpMyAdmin 2.11.x < 2.11.9.4 / 3.0.x < 3.1.3 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.800381 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References CVE: CVE-2009-1148, CVE-2009-1149, CVE-2009-1150, CVE-2009-1151 BID:34251, 34253, 34236 Other: URL:http://secunia.com/advisories/34430 URL:http://www.phpmyadmin.net/home_page/security/PMASA-2009-1.php URL:http://www.phpmyadmin.net/home_page/security/PMASA-2009-2.php URL:http://www.phpmyadmin.net/home_page/security/PMASA-2009-3.php

High (CVSS: 7.5) NVT: phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 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.
Vulnerability Detection Result Installed version: 3.1.1 Fixed version: 3.1.3.1
Impact 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.
Solution Solution type: VendorFix Update to version 3.1.3.1 or later.
Affected Software/OS Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.
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: 14031 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References CVE: CVE-2009-1148, CVE-2009-1149 BID:34253 Other: URL: http://www.securityfocus.com/bid/34253
... continues on next page ...

...continued from previous page ...

High (CVSS: 7.5)**NVT: phpMyAdmin Code Injection and XSS Vulnerability****Product detection result**

cpe:/a:phpmyadmin:phpmyadmin:3.1.1

Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary

phpMyAdmin is prone to a remote PHP code-injection vulnerability and to a cross-site scripting vulnerability.

Vulnerability Detection Result

Installed version: 3.1.1

Fixed version: 2.11.9.5 / 3.1.3.1

Impact

An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system. Other attacks are also possible.

Solution**Solution type:** VendorFix

Update to version 2.11.9.5 / 3.1.3.1 or later.

Affected Software/OS

Versions prior to phpMyAdmin 2.11.9.5 and 3.1.3.1 are vulnerable.

Vulnerability Detection Method

Details: phpMyAdmin Code Injection and XSS Vulnerability

OID:1.3.6.1.4.1.25623.1.0.100077

Version used: \$Revision: 14031 \$

Product Detection Result

Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1

Method: phpMyAdmin Detection

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

CVE: CVE-2009-1151

BID:34236, 34251

Other:

URL:<http://www.securityfocus.com/bid/34236>URL:<http://www.securityfocus.com/bid/34251>

<p>High (CVSS: 10.0) NVT: phpMyAdmin End of Life Detection (Linux)</p>
<p>Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p>Summary The phpMyAdmin version on the remote host has reached the end of life and should not be used anymore.</p>
<p>Vulnerability Detection Result The "phpMyAdmin" version on the remote host has reached the end of life. CPE: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Installed version: 3.1.1 Location/URL: http://10.0.2.4/phpMyAdmin EOL version: 3.1 EOL date: unknown</p>
<p>Impact An end of life version of phpMyAdmin 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.</p>
<p>Solution Solution type: VendorFix Update the phpMyAdmin version on the remote host to a still supported version.</p>
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: phpMyAdmin End of Life Detection (Linux) OID:1.3.6.1.4.1.25623.1.0.113015 Version used: \$Revision: 11982 \$</p>
<p>Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p>References Other: URL:https://www.phpmyadmin.net/downloads/ URL:https://www.phpmyadmin.net/news/2011/7/12/phpmyadmin-211-end-of-life/ URL:https://www.phpmyadmin.net/news/2017/1/23/phpmyadmin-466-441510-and-40101-40102-are-released/</p>

High (CVSS: 7.5) NVT: phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary phpMyAdmin is prone to SQL-injection and cross-site scripting vulnerabilities because it fails to sufficiently sanitize user-supplied data.
Vulnerability Detection Result Installed version: 3.1.1 Fixed version: See references
Impact Exploiting these issues could allow an attacker to steal cookie- based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.
Solution Solution type: VendorFix Vendor updates are available. Please see the references for details.
Affected Software/OS Versions prior to phpMyAdmin 2.11.9.6 and 3.2.2.1 are affected.
Vulnerability Detection Method Details: phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100307 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References CVE: CVE-2009-3696, CVE-2009-3697 BID:36658 Other: URL:http://www.securityfocus.com/bid/36658 URL:http://www.phpmyadmin.net/ URL:http://freshmeat.net/projects/phpmyadmin/releases/306669 URL:http://freshmeat.net/projects/phpmyadmin/releases/306667

High (CVSS: 7.5) NVT: Test HTTP dangerous methods
Summary Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files.
Vulnerability Detection Result We could upload the following files via the PUT method at this web server: <code>http://10.0.2.4/dav/puttest1227244251.html</code> We could delete the following files via the DELETE method at this web server: <code>http://10.0.2.4/dav/puttest1227244251.html</code>
Impact - Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server. - Enabled DELETE method: This might allow an attacker to delete additional files on this web server.
Solution Solution type: Mitigation Use access restrictions to these dangerous HTTP methods or disable them completely.
Vulnerability Detection Method Details: Test HTTP dangerous methods OID:1.3.6.1.4.1.25623.1.0.10498 Version used: \$Revision: 9335 \$
References BID:12141 Other: OWASP:OWASP-CM-001

High (CVSS: 7.5) NVT: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities
Product detection result <code>cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5</code> Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.↔0.901001)
Summary Tiki Wiki CMS Groupware is prone to multiple unspecified vulnerabilities, including: <ul style="list-style-type: none"> - An unspecified SQL-injection vulnerability - An unspecified authentication-bypass vulnerability ... continues on next page ...

...continued from previous page...
- An unspecified vulnerability
Vulnerability Detection Result Installed version: 1.9.5 Fixed version: 4.2
Impact Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible.
Solution Solution type: VendorFix The vendor has released an advisory and fixes. Please see the references for details.
Affected Software/OS Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.
Vulnerability Detection Method Details: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100537 Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Method: Tiki Wiki CMS Groupware Version Detection OID: 1.3.6.1.4.1.25623.1.0.901001)
References CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136 BID:38608 Other: URL:http://www.securityfocus.com/bid/38608 URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=247 ↪34 URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=250 ↪46 URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254 ↪24 URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254 ↪35 URL:http://info.tikiwiki.org/article86-Tiki-Announces-3-5-and-4-2-Releases URL:http://info.tikiwiki.org/tiki-index.php?page=homepage

High (CVSS: 10.0) NVT: TWiki XSS and Command Execution Vulnerabilities
Product detection result cpe:/a:twiki:twiki:01.Feb.2003 Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
Summary The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 4.2.4
Impact Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.
Solution Solution type: VendorFix Upgrade to version 4.2.4 or later.
Affected Software/OS TWiki, TWiki version prior to 4.2.4.
Vulnerability Insight The flaws are due to, - %URLPARAM}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack. - %SEARCH}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.
Vulnerability Detection Method Details: TWiki XSS and Command Execution Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.800320 Version used: \$Revision: 12952 \$
Product Detection Result Product: cpe:/a:twiki:twiki:01.Feb.2003 Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)
References CVE: CVE-2008-5304, CVE-2008-5305 BID:32668, 32669 ... continues on next page ...

...continued from previous page...

Other:URL:<http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304>URL:<http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5305>[\[return to 10.0.2.4 \]](#)**High 2121/tcp****High (CVSS: 10.0)****NVT: ProFTPD Multiple Remote Vulnerabilities****Product detection result**

cpe:/a:proftpd:proftpd:1.3.1

Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.↪0.900815)

Summary

The host is running ProFTPD and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 1.3.1

Fixed version: 1.3.3c

Impact

Successful exploitation may allow execution of arbitrary code or cause a denial-of-service.

Solution**Solution type:** VendorFix

Upgrade to ProFTPD version 1.3.3c or later.

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: 13602 \$

...continues on next page...

...continued from previous page ...
Product Detection Result Product: cpe:/a:proftpd:proftpd:1.3.1 Method: ProFTPD Server Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.900815)
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/ URL:http://www.proftpd.org/

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:1.3.1 Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.↪0.900815)
Summary ProFTPD is prone to a remote code-execution vulnerability.
Vulnerability Detection Result Installed version: 1.3.1 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
... continues on next page ...

...continued from previous page ...
Version used: \$Revision: 11997 \$
Product Detection Result Product: cpe:/a:proftpd:proftpd:1.3.1 Method: ProFTPD Server Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.900815)
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: 7.5) NVT: ProFTPD Server SQL Injection Vulnerability
Product detection result cpe:/a:proftpd:proftpd:1.3.1 Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.↔0.900815)
Summary This host is running ProFTPD Server and is prone to remote SQL Injection vulnerability.
Vulnerability Detection Result Installed version: 1.3.1 Fixed version: 1.3.2rc3
Impact Successful exploitation will allow remote attackers to execute arbitrary SQL commands, thus gaining access to random user accounts.
Solution Solution type: VendorFix Upgrade to the latest version 1.3.2rc3.
Affected Software/OS ProFTPD Server version 1.3.1 through 1.3.2rc2.
Vulnerability Insight This flaw occurs because the server performs improper input sanitising, ... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - when a %(percent) character is passed in the username, a single quote (') gets introduced during variable substitution by mod_sql and this eventually allows for an SQL injection during login. - when NLS support is enabled, a flaw in variable substitution feature in mod_sql_mysql and mod_sql_postgres may allow an attacker to bypass SQL injection protection mechanisms via invalid, encoded multibyte characters.
Vulnerability Detection Method Details: ProFTPD Server SQL Injection Vulnerability OID:1.3.6.1.4.1.25623.1.0.900507 Version used: \$Revision: 13602 \$
Product Detection Result Product: cpe:/a:proftpd:proftpd:1.3.1 Method: ProFTPD Server Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.900815)
References CVE: CVE-2009-0542, CVE-2009-0543 BID:33722 Other: URL:http://www.milw0rm.com/exploits/8037 URL:http://www.securityfocus.com/archive/1/archive/1/500833/100/0/threaded URL:http://www.securityfocus.com/archive/1/archive/1/500851/100/0/threaded

[\[return to 10.0.2.4 \]](#)

High 513/tcp

High (CVSS: 7.5) NVT: rlogin Passwordless / Unencrypted Cleartext Login
Summary This remote host is running a rlogin service.
Vulnerability Detection Result The service is misconfigured so it is allowing connections without a password.
Solution Solution type: Mitigation Disable the rlogin service and use alternatives like SSH instead.
Vulnerability Insight rlogin has several serious security problems, <ul style="list-style-type: none"> - all information, including passwords, is transmitted unencrypted. - .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password) ... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Details: rlogin Passwordless / Unencrypted Cleartext Login

OID:1.3.6.1.4.1.25623.1.0.901202

Version used: \$Revision: 13541 \$

References**Other:**URL:<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651>URL:<http://en.wikipedia.org/wiki/Rlogin>URL:<http://www.ietf.org/rfc/rfc1282.txt>[\[return to 10.0.2.4 \]](#)**High 3306/tcp**

High (CVSS: 8.5)

NVT: MySQL 'sql_parse.cc' Multiple Format String Vulnerabilities

Product detection result

cpe:/a:mysql:mysql:5.0.51a

Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

Summary

The host is running MySQL and is prone to Multiple Format String vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation could allow remote authenticated users to cause a Denial of Service and possibly have unspecified other attacks.

Solution**Solution type:** VendorFixUpgrade to MySQL version 5.1.36 or later <http://dev.mysql.com/downloads>**Affected Software/OS**

MySQL version 4.0.0 to 5.0.83 on all running platform.

Vulnerability Insight

The flaws are due to error in the 'dispatch_command' function in sql_parse.cc in libmysqld/ which can caused via format string specifiers in a database name in a 'COM_CREATE_DB' or 'COM_DROP_DB' request.

... continues on next page ...

...continued from previous page...

Vulnerability Detection Method

Details: MySQL 'sql_parse.cc' Multiple Format String Vulnerabilities

OID:1.3.6.1.4.1.25623.1.0.800842

Version used: \$Revision: 11554 \$

Product Detection Result

Product: cpe:/a:mysql:mysql:5.0.51a

Method: MySQL/MariaDB Detection

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

CVE: CVE-2009-2446

BID:35609

Other:

URL:<http://secunia.com/advisories/35767>URL:<http://xforce.iss.net/xforce/xfdb/51614>URL:<http://www.securityfocus.com/archive/1/archive/1/504799/100/0/threaded>

High (CVSS: 9.0)

NVT: MySQL / MariaDB weak password

Product detection result

cpe:/a:mysql:mysql:5.0.51a

Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

Summary

It was possible to login into the remote MySQL as root using weak credentials.

Vulnerability Detection Result

It was possible to login as root with an empty password.

Solution**Solution type:** Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: MySQL / MariaDB weak password

OID:1.3.6.1.4.1.25623.1.0.103551

Version used: \$Revision: 12175 \$

Product Detection Result

Product: cpe:/a:mysql:mysql:5.0.51a

Method: MySQL/MariaDB Detection

OID: 1.3.6.1.4.1.25623.1.0.100152)

High (CVSS: 7.5) NVT: MySQL 5.0.51a Unspecified Remote Code Execution Vulnerability
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary MySQL 5.0.51a is prone to an unspecified remote code-execution vulnerability.
Vulnerability Detection Result Installed version: 5.0.51a Fixed version: Unknown
Impact An attacker can leverage this issue to execute arbitrary code within the context of the vulnerable application. Failed exploit attempts will result in a denial-of-service condition.
Solution Solution type: WillNotFix No known solution was made available for at least one year since the 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 This issue affects MySQL 5.0.51a. Other versions may also be vulnerable.
Vulnerability Insight Very few technical details are currently available.
Vulnerability Detection Method Details: MySQL 5.0.51a Unspecified Remote Code Execution Vulnerability OID:1.3.6.1.4.1.25623.1.0.100436 Version used: \$Revision: 11830 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2009-4484 BID:37640 Other: URL:http://www.securityfocus.com/bid/37640 URL:http://archives.neohapsis.com/archives/dailydave/2010-q1/0002.html
... continues on next page ...

...continued from previous page ...

URL: <http://www.mysql.com/>
 URL: http://intevydis.com/mysql_demo.html

High (CVSS: 9.3)**NVT: MySQL 5.x Unspecified Buffer Overflow Vulnerability****Product detection result**

cpe:/a:mysql:mysql:5.0.51a

Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

Summary

MySQL is prone to a buffer-overflow vulnerability because it fails to perform adequate boundary checks on user-supplied data.

Vulnerability Detection Result

Installed version: 5.0.51a

Fixed version: Unknown

Impact

An attacker can leverage this issue to execute arbitrary code within the context of the vulnerable application. Failed exploit attempts will result in a denial-of-service condition.

Solution**Solution type:** WillNotFix

No known solution was made available for at least one year since the 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

This issue affects MySQL 5.x. Other versions may also be vulnerable.

Vulnerability Detection Method

Details: MySQL 5.x Unspecified Buffer Overflow Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.100271

Version used: \$Revision: 11830 \$

Product Detection Result

Product: cpe:/a:mysql:mysql:5.0.51a

Method: MySQL/MariaDB Detection

OID: 1.3.6.1.4.1.25623.1.0.100152)

References

BID: 36242

Other:

... continues on next page ...

...continued from previous page...

URL:<http://www.securityfocus.com/bid/36242>
 URL:<http://www.mysql.com/>

High (CVSS: 10.0)**NVT: MySQL End Of Life Detection (Linux)****Product detection result**

cpe:/a:mysql:mysql:5.0.51a

Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

Summary

The MySQL version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

The "MySQL" version on the remote host has reached the end of life.

CPE: cpe:/a:mysql:mysql:5.0.51a

Installed version: 5.0.51a

EOL version: 5.0

EOL date: 2012-01-09

Impact

An end of life version of MySQL 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 MySQL version on the remote host to a still supported version.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: MySQL End Of Life Detection (Linux)

OID:1.3.6.1.4.1.25623.1.0.108190

Version used: \$Revision: 12175 \$

Product Detection Result

Product: cpe:/a:mysql:mysql:5.0.51a

Method: MySQL/MariaDB Detection

OID: 1.3.6.1.4.1.25623.1.0.100152)

References**Other:**URL:<https://www.mysql.com/support/eol-notice.html>URL:https://en.wikipedia.org/wiki/MySQL#Release_history

<p>High (CVSS: 7.5) NVT: MySQL Server Buffer Overflow Vulnerability (Linux)</p>
<p>Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>Summary The host is running MySQL and is prone to Buffer overflow Vulnerability</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Impact Successful exploitation could allow attackers to execute arbitrary code.</p>
<p>Solution Solution type: VendorFix Upgrade to MySQL Version 5.0.90 or 5.1.43 or 5.5.1 or later.</p>
<p>Affected Software/OS MySQL Version 5.0.x before 5.0.90, MySQL version 5.1.x before 5.1.43, MySQL 5.5.x through 5.5.0-m2 On Linux</p>
<p>Vulnerability Insight The flaw is due to an error in application that allows remote attackers to execute arbitrary code via unspecified vectors</p>
<p>Vulnerability Detection Method Details: MySQL Server Buffer Overflow Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.901093 Version used: \$Revision: 13960 \$</p>
<p>Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>References CVE: CVE-2009-4484 Other: URL:http://secunia.com/advisories/38364 URL:http://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-1.html URL:http://dev.mysql.com/doc/relnotes/mysql/5.1/en/news-5-1-43.html URL:http://dev.mysql.com/doc/relnotes/mysql/5.0/en/news-5-0-90.html URL:http://dev.mysql.com/downloads</p>

[\[return to 10.0.2.4 \]](#)

High 1524/tcp

High (CVSS: 10.0) NVT: Possible Backdoor: Ingreslock
Summary A backdoor is installed on the remote host
Vulnerability Detection Result The service is answering to an 'id;' command with the following response: uid=0(↪root) gid=0(root)
Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.
Solution Solution type: Workaround
Vulnerability Detection Method Details: Possible Backdoor: Ingreslock OID:1.3.6.1.4.1.25623.1.0.103549 Version used: \$Revision: 11327 \$

[\[return to 10.0.2.4 \]](#)

High 5432/tcp

High (CVSS: 7.5) NVT: PostgreSQL < 10.6, 11.x < 11.1 SQL Injection Vulnerability (Linux)
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary PostgreSQL is prone to an SQL injection vulnerability.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: 10.6
... continues on next page ...

...continued from previous page ...
Solution Solution type: VendorFix Update to version 10.6 or 11.1 respectively.
Affected Software/OS PostgreSQL before versions 10.6 and 11.1.
Vulnerability Insight A SQL Injection flaw has been discovered in PostgreSQL server in the way triggers that enable transition relations are dumped. The transition relation name is not correctly quoted and it may allow an attacker with CREATE privilege on some non-temporary schema or TRIGGER privilege on some table to create a malicious trigger that, when dumped and restored, would result in additional SQL statements being executed.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PostgreSQL < 10.6, 11.x < 11.1 SQL Injection Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.112429 Version used: \$Revision: 12858 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2018-16850 Other: URL: https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-16850 URL: https://www.postgresql.org/about/news/1905/

High (CVSS: 10.0)
NVT: PostgreSQL End Of Life Detection (Linux)

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary
The PostgreSQL version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The "PostgreSQL" version on the remote host has reached the end of life.
CPE: cpe:/a:postgresql:postgresql:8.3.1

... continues on next page ...

...continued from previous page ...
Installed version: 8.3.1 EOL version: 8.3 EOL date: 2013-02-01
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 Checks if a vulnerable version is present on the target host. Details: PostgreSQL End Of Life Detection (Linux) OID:1.3.6.1.4.1.25623.1.0.140158 Version used: \$Revision: 11874 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References Other: URL: https://www.postgresql.org/support/versioning/

High (CVSS: 8.5)
 NVT: PostgreSQL Multiple Security Vulnerabilities

Product detection result
 cpe:/a:postgresql:postgresql:8.3.1
 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary
 PostgreSQL is prone to multiple security vulnerabilities.

Vulnerability Detection Result
 Installed version: 8.3.1
 Fixed version: See references

Impact
 ... continues on next page ...

...continued from previous page ...
Attackers can exploit these issues to bypass certain security restrictions and execute arbitrary Perl or Tcl code.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS These issues affect versions prior to the following PostgreSQL versions: 8.4.4 8.3.11 8.2.17 8.1.21 8.0.25 7.4.29
Vulnerability Detection Method Details: PostgreSQL Multiple Security Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100645 Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2010-1169, CVE-2010-1170, CVE-2010-1447 BID:40215 Other: URL: http://www.securityfocus.com/bid/40215 URL: http://www.postgresql.org/about/news.1203 URL: http://www.postgresql.org/ URL: http://www.postgresql.org/support/security
High (CVSS: 9.0) NVT: PostgreSQL Multiple Vulnerabilities - Mar15 (Linux)
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary This host is running PostgreSQL and is prone to multiple vulnerabilities.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: 9.1.20
Impact Successful exploitation will allow a remote attacker to escalate privileges and to cause denial of service conditions.
Solution Solution type: VendorFix Upgrade to version 9.1.20 or 9.2.15 or 9.3.11 or 9.4.6 or 9.5.1 or higher.
Affected Software/OS PostgreSQL version before 9.1.20, 9.2.x before 9.2.15, 9.3.x before 9.3.11, 9.4.x before 9.4.6, and 9.5.x before 9.5.1 on Linux.
Vulnerability Insight Multiple flaws are due to the PostgreSQL incorrectly handle certain regular expressions and certain configuration settings (GUCS) for users of PL/Java.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PostgreSQL Multiple Vulnerabilities - Mar15 (Linux) OID:1.3.6.1.4.1.25623.1.0.807518 Version used: \$Revision: 12455 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2016-0773, CVE-2016-0766 BID:83184 Other: URL: http://www.ubuntu.com/usn/USN-2894-1 URL: http://www.postgresql.org/about/news/1644 URL: http://www.postgresql.org/download
High (CVSS: 9.0) NVT: PostgreSQL weak password
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
... continues on next page ...

...continued from previous page ...
Summary It was possible to login into the remote PostgreSQL as user postgres using weak credentials.
Vulnerability Detection Result It was possible to login as user postgres with password "postgres".
Solution Solution type: Mitigation Change the password as soon as possible.
Vulnerability Detection Method Details: PostgreSQL weak password OID:1.3.6.1.4.1.25623.1.0.103552 Version used: \$Revision: 10312 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)

[\[return to 10.0.2.4 \]](#)

High 6200/tcp

High (CVSS: 7.5) NVT: vsftpd Compromised Source Packages Backdoor Vulnerability
Summary vsftpd is prone to a backdoor vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
Solution Solution type: VendorFix The repaired package can be downloaded from the referenced link. Please validate the package with its signature.
Affected Software/OS The vsftpd 2.3.4 source package is affected.
... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Details: vsftpd Compromised Source Packages Backdoor Vulnerability

OID:1.3.6.1.4.1.25623.1.0.103185

Version used: \$Revision: 12076 \$

References

BID:48539

Other:

URL:http://www.securityfocus.com/bid/48539

URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↳doored.html

URL:https://security.appspot.com/vsftpd.html

[\[return to 10.0.2.4 \]](#)**High 445/tcp**

High (CVSS: 7.5)

NVT: Samba 'mount.cifs' Utility Symlink Attack Local Privilege Escalation Vulnerability

Product detection result

cpe:/a:samba:samba:3.0.20

Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary

Samba is prone to a local privilege-escalation vulnerability in the 'mount.cifs' utility.

Vulnerability Detection Result

Installed version: 3.0.20

Fixed version: 3.0.38/3.3.13/3.4.8

Installation

path / port: 445/tcp

Impact

Local attackers can exploit this issue to gain elevated privileges on affected computers.

Solution**Solution type:** VendorFix

Updates are available. Please see the references for more information.

Vulnerability Detection Method

Details: Samba 'mount.cifs' Utility Symlink Attack Local Privilege Escalation Vulnerabil.

↳..

OID:1.3.6.1.4.1.25623.1.0.100623

...continues on next page ...

...continued from previous page ...
Version used: \$Revision: 10398 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2010-0747 BID: 39898 Other: URL: http://www.securityfocus.com/bid/39898 URL: http://www.samba.org

High (CVSS: 7.5) NVT: Samba 'mtab' Lock File Handling Local Denial of Service Vulnerability
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary Samba is prone to a local denial-of-service vulnerability that affects the mounting utilities 'mount.cifs' and 'umount.cifs'.
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 3.6.1 Installation path / port: 445/tcp
Impact A local attacker can exploit this issue to cause the mounting utilities to abort, resulting in a denial-of-service condition.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Vulnerability Detection Method Details: Samba 'mtab' Lock File Handling Local Denial of Service Vulnerability OID: 1.3.6.1.4.1.25623.1.0.103283 Version used: \$Revision: 10398 \$
... continues on next page ...

...continued from previous page ...
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2011-3585 BID: 49940 Other: URL: http://www.securityfocus.com/bid/49940 URL: https://bugzilla.samba.org/show_bug.cgi?id=7179 URL: http://git.samba.org/?p=cifs-utils.git;a=commitdiff;h=810f7e4e0f2dbcbee02↵94d9b371071cb08268200 URL: http://us1.samba.org/samba/

High (CVSS: 7.5) NVT: Samba 'SMB1 Packet Chaining' Unspecified Remote Memory Corruption Vulnerability
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary Samba is prone to an unspecified memory-corruption vulnerability.
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 3.3.13 Installation path / port: 445/tcp
Impact Attackers can exploit this issue to execute arbitrary code in the context of the application. Failed attacks may cause a denial-of-service condition.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS Samba versions prior to 3.3.13 are vulnerable.
Vulnerability Detection Method Details: Samba 'SMB1 Packet Chaining' Unspecified Remote Memory Corruption Vulnerability OID: 1.3.6.1.4.1.25623.1.0.100680
... continues on next page ...

...continued from previous page ...
Version used: \$Revision: 10398 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2010-2063 BID: 40884 Other: URL: https://www.securityfocus.com/bid/40884 URL: http://www.samba.org URL: http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=873 URL: http://www.samba.org/samba/security/CVE-2010-2063.html

High (CVSS: 10.0) NVT: Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 3.6.25 or 4.0.25 or 4.1.17, 4.2.0rc5, or later Installation path / port: 445/tcp
Impact An attacker can exploit this issue to execute arbitrary code with root privileges. Failed exploit attempts will cause a denial-of-service condition
Solution Solution type: VendorFix Updates are available. Please see the references or vendor advisory for more information.
Affected Software/OS Samba 3.5.x and 3.6.x before 3.6.25, 4.0.x before 4.0.25, 4.1.x before 4.1.17, and 4.2.x before 4.2.0rc5
... continues on next page ...

...continued from previous page ...
Vulnerability Insight The Netlogon server implementation in smbd performs a free operation on an uninitialized stack pointer, which allows remote attackers to execute arbitrary code via crafted Netlogon packets that use the ServerPasswordSet RPC API, as demonstrated by packets reaching the _netr_ServerPasswordSet function in rpc_server/netlogon/srv_netlog_nt.c.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability OID:1.3.6.1.4.1.25623.1.0.105231 Version used: \$Revision: 12106 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2015-0240 BID:72711 Other: URL:http://www.securityfocus.com/bid/72711 URL:http://www.samba.org

High (CVSS: 10.0)

NVT: Samba End Of Life Detection

Product detection result

cpe:/a:samba:samba:3.0.20

Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary

The Samba version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

The "Samba" version on the remote host has reached the end of life.

CPE: cpe:/a:samba:samba:3.0.20

Installed version: 3.0.20

Location/URL: 445/tcp

EOL version: 3.0

EOL date: 2009-08-05

Impact

... continues on next page ...

...continued from previous page ...
An end of life version of Samba 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 Samba version on the remote host to a still supported version.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba End Of Life Detection OID:1.3.6.1.4.1.25623.1.0.140159 Version used: \$Revision: 11923 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References Other: URL: https://wiki.samba.org/index.php/Samba_Release_Planning

High (CVSS: 7.5) NVT: Samba SID Parsing Remote Buffer Overflow Vulnerability
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary Samba is prone to a remote stack-based buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it to an insufficiently sized memory buffer.
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 3.5.5 Installation path / port: 445/tcp
Impact An attacker can exploit this issue to execute arbitrary code in the context of the affected application. Failed exploit attempts will likely result in a denial of service.
Solution ... continues on next page ...

...continued from previous page ...
Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS Samba versions prior to 3.5.5 are vulnerable.
Vulnerability Detection Method Details: Samba SID Parsing Remote Buffer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.100803 Version used: \$Revision: 10398 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2010-3069 BID:43212 Other: URL:https://www.securityfocus.com/bid/43212 URL:http://us1.samba.org/samba/history/samba-3.5.5.html URL:http://www.samba.org URL:http://us1.samba.org/samba/security/CVE-2010-2069.html

[\[return to 10.0.2.4 \]](#)

High 5900/tcp

High (CVSS: 9.0) NVT: VNC Brute Force Login
Summary Try to log in with given passwords via VNC protocol.
Vulnerability Detection Result It was possible to connect to the VNC server with the password: password
Solution Solution type: Mitigation Change the password to something hard to guess or enable password protection at all.
Vulnerability Insight This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all.
... continues on next page ...

...continued from previous page ...
Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked. Note as well that passwords can be max. 8 characters long.
Vulnerability Detection Method Details: VNC Brute Force Login OID:1.3.6.1.4.1.25623.1.0.106056 Version used: \$Revision: 13328 \$

[\[return to 10.0.2.4 \]](#)

Medium 25/tcp

Medium (CVSS: 5.0) NVT: Check if Mailserver answer to VRFY and EXPN requests
Summary The Mailserver on this host answers to VRFY and/or EXPN requests.
Vulnerability Detection Result 'VRFY root' produces the following answer: 252 2.0.0 root
Solution Solution type: Workaround Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
Vulnerability Insight VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.
Vulnerability Detection Method Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: \$Revision: 13470 \$
References Other: URL: http://cr.yp.to/smtp/vrfy.html

<p>Medium (CVSS: 6.8)</p> <p>NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability</p>
<p>Summary</p> <p>Multiple vendors' implementations of 'STARTTLS' are prone to a vulnerability that lets attackers inject arbitrary commands.</p>
<p>Vulnerability Detection Result</p> <p>Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Impact</p> <p>An attacker can exploit this issue to execute arbitrary commands in the context of the user running the application. Successful exploits can allow attackers to obtain email usernames and passwords.</p>
<p>Solution</p> <p>Solution type: VendorFix</p> <p>Updates are available. Please see the references for more information.</p>
<p>Affected Software/OS</p> <p>The following vendors are affected:</p> <p>Ipswitch Kerio Postfix Qmail-TLS Oracle SCO Group spamdyke ISC</p>
<p>Vulnerability Detection Method</p> <p>Send a special crafted 'STARTTLS' request and check the response.</p> <p>Details: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection . ↔...</p> <p>OID:1.3.6.1.4.1.25623.1.0.103935</p> <p>Version used: \$Revision: 13204 \$</p>
<p>References</p> <p>CVE: CVE-2011-0411, CVE-2011-1430, CVE-2011-1431, CVE-2011-1432, CVE-2011-1506, ↔CVE-2011-1575, CVE-2011-1926, CVE-2011-2165</p> <p>BID:46767</p> <p>Other:</p> <p>URL:http://www.securityfocus.com/bid/46767</p> <p>URL:http://kolab.org/pipermail/kolab-announce/2011/000101.html</p> <p>URL:http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424</p> <p>URL:http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7</p> <p>URL:http://www.kb.cert.org/vuls/id/MAPG-8D9M4P</p>
<p>... continues on next page ...</p>

...continued from previous page ...
URL:http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release- ↪notes.txt URL:http://www.postfix.org/CVE-2011-0411.html URL:http://www.pureftpd.org/project/pure-ftpd/news URL:http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNot ↪es_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf URL:http://www.spamdyke.org/documentation/Changelog.txt URL:http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?inclu ↪de_text=1 URL:http://www.securityfocus.com/archive/1/516901 URL:http://support.avaya.com/css/P8/documents/100134676 URL:http://support.avaya.com/css/P8/documents/100141041 URL:http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html URL:http://inoa.net/qmail-tls/vu555316.patch URL:http://www.kb.cert.org/vuls/id/555316

Medium (CVSS: 4.3)

NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

Summary

This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result

'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA

TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA

TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

Impact

Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution

Solution type: VendorFix

- Remove support for 'DHE_EXPORT' cipher suites from the service

- If running OpenSSL update to version 1.0.2b or 1.0.1n or later.

Affected Software/OS

- Hosts accepting 'DHE_EXPORT' cipher suites

- OpenSSL version before 1.0.2b and 1.0.1n

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.
Vulnerability Detection Method Check previous collected cipher suites saved in the KB. Details: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) OID:1.3.6.1.4.1.25623.1.0.805188 Version used: \$Revision: 11872 \$
References CVE: CVE-2015-4000 BID:74733 Other: URL:https://weakdh.org URL:https://weakdh.org/imperfect-forward-secrecy.pdf URL:http://openwall.com/lists/oss-security/2015/05/20/8 URL:https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained URL:https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-change ↪s

Medium (CVSS: 5.0) NVT: SSL/TLS: Certificate Expired
Summary The remote server's SSL/TLS certificate has already expired.
Vulnerability Detection Result The certificate of the remote service expired on 2010-04-16 14:07:45. Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6 ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6 ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX serial: 00FAF93A4C7FB6B9CC valid from : 2010-03-17 14:07:45 UTC valid until: 2010-04-16 14:07:45 UTC fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436 ↪DE813CC
Solution ... continues on next page ...

...continued from previous page ...
Solution type: Mitigation Replace the SSL/TLS certificate by a new one.
Vulnerability Insight This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.
Vulnerability Detection Method Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: \$Revision: 11103 \$
Medium (CVSS: 4.3) NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
Summary It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
Vulnerability Detection Result In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and S↔SLv3 protocols and supports one or more ciphers. Those supported ciphers can b↔e found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.↔25623.1.0.802067) NVT.
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Solution Solution type: Mitigation It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.
Affected Software/OS All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
Vulnerability Insight The SSLv2 and SSLv3 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)
Vulnerability Detection Method Check the used protocols of the services provided by this system. Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
... continues on next page ...

...continued from previous page ...	
OID:1.3.6.1.4.1.25623.1.0.111012 Version used: \$Revision: 5547 \$	
References CVE: CVE-2016-0800, CVE-2014-3566 Other: URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report URL:https://bettercrypto.org/ URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/ URL:https://drownattack.com/ URL:https://www.imperialviolet.org/2014/10/14/poodle.html	
Medium (CVSS: 4.0) NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	
Summary The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).	
Vulnerability Detection Result Server Temporary Key Size: 1024 bits	
Impact An attacker might be able to decrypt the SSL/TLS communication offline.	
Solution Solution type: Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.	
Vulnerability Insight The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.	
Vulnerability Detection Method Checks the DHE temporary public key size. Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↪... OID:1.3.6.1.4.1.25623.1.0.106223 Version used: \$Revision: 12865 \$	
References ... continues on next page ...	

...continued from previous page ...

Other:URL: <https://weakdh.org/>URL: <https://weakdh.org/sysadmin.html>

Medium (CVSS: 4.3)

NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

Summary

This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result

'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5

TLS_RSA_EXPORT_WITH_RC4_40_MD5

'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5

TLS_RSA_EXPORT_WITH_RC4_40_MD5

Impact

Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution**Solution type:** VendorFix

- Remove support for 'RSA_EXPORT' cipher suites from the service.

- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

Affected Software/OS

- Hosts accepting 'RSA_EXPORT' cipher suites

- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

Vulnerability Insight

Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

Vulnerability Detection Method

Check previous collected cipher suites saved in the KB.

Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

OID:1.3.6.1.4.1.25623.1.0.805142

Version used: \$Revision: 11872 \$

... continues on next page ...

... continued from previous page ...	
References CVE: CVE-2015-0204 BID: 71936 Other: URL: https://freakattack.com URL: http://secpod.org/blog/?p=3818 URL: http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-fc21936-actoring-nsa.html URL: https://www.openssl.org	
Medium (CVSS: 4.3) NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	
Summary This host is prone to an information disclosure vulnerability.	
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.	
Impact Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.	
Solution Solution type: Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+	
Vulnerability Insight The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code	
Vulnerability Detection Method Evaluate previous collected information about this service. Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↳.. OID: 1.3.6.1.4.1.25623.1.0.802087 Version used: \$Revision: 11402 \$	
References CVE: CVE-2014-3566 BID: 70574 Other:	
... continues on next page ...	

...continued from previous page ...
URL: https://www.openssl.org/~bodo/ssl-poodle.pdf URL: https://www.imperialviolet.org/2014/10/14/poodle.html URL: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html URL: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit-ing-ssl-30.html

[\[return to 10.0.2.4 \]](#)

Medium general/tcp

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 Solution type: VendorFix 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: 11066 \$
References CVE: CVE-2004-0230 BID:10183 Other: URL: http://xforce.iss.net/xforce/xfdb/15886
... continues on next page ...

...continued from previous page ...
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.msp
URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.msp
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

[\[return to 10.0.2.4 \]](#)

Medium 23/tcp

Medium (CVSS: 4.8) NVT: Telnet Unencrypted Cleartext Login
Summary The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.
Solution Solution type: Mitigation Replace Telnet with a protocol like SSH which supports encrypted connections.
Vulnerability Detection Method Details: Telnet Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108522 Version used: \$Revision: 13620 \$

[\[return to 10.0.2.4 \]](#)

Medium 21/tcp

Medium (CVSS: 6.4) NVT: Anonymous FTP Login Reporting
Summary Reports if the remote FTP Server allows anonymous logins.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result It was possible to login to the remote FTP service with the following anonymous ↵account(s): anonymous:anonymous@example.com ftp:anonymous@example.com
Impact Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to: - gain access to sensitive files - upload or delete files.
Solution Solution type: Mitigation If you do not want to share files, you should disable anonymous logins.
Vulnerability Insight A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.
Vulnerability Detection Method Details: Anonymous FTP Login Reporting OID:1.3.6.1.4.1.25623.1.0.900600 Version used: \$Revision: 12030 \$
References Other: URL: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497
Medium (CVSS: 4.8) NVT: FTP Unencrypted Cleartext Login
Summary The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
Vulnerability Detection Result The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↵. Response(s): Anonymous sessions: 331 Please specify the password. Non-anonymous sessions: 331 Please specify the password.
... continues on next page ...

...continued from previous page ...
Impact An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
Solution Solution type: Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
Vulnerability Detection Method Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108528 Version used: \$Revision: 13611 \$
Medium (CVSS: 5.1) NVT: vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability
Product detection result cpe:/a:beasts:vsftpd:2.3.4 Detected by vsFTPd FTP Server Detection (OID: 1.3.6.1.4.1.25623.1.0.111050)
Summary vsftpd is prone to a buffer-overflow vulnerability because it fails to perform adequate boundary checks on user-supplied data.
Vulnerability Detection Result Installed version: 2.3.4 Fixed version: 2.3.5
Impact Attackers may leverage this issue to execute arbitrary code in the context of the application. Failed attacks will cause denial-of-service conditions.
Solution Solution type: VendorFix A fixed version 2.3.5 is available. Please see the references for more information.
Affected Software/OS vsftpd 2.3.4 is affected. Other versions may also be vulnerable.
Vulnerability Detection Method Details: vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.103362 ... continues on next page ...

...continued from previous page ...
Version used: \$Revision: 12018 \$
Product Detection Result Product: cpe:/a:beasts:vsftpd:2.3.4 Method: vsFTPD FTP Server Detection OID: 1.3.6.1.4.1.25623.1.0.111050)
References BID:51013 Other: URL:http://www.securityfocus.com/bid/51013 URL:http://dividead.wordpress.com/tag/heap-overflow/ URL:https://security.appspot.com/vsftpd/Changelog.txt URL:https://security.appspot.com/vsftpd.html

Medium (CVSS: 5.0) NVT: vsftpd < 3.0.3 Security Bypass Vulnerability
Product detection result cpe:/a:beasts:vsftpd:2.3.4 Detected by vsFTPD FTP Server Detection (OID: 1.3.6.1.4.1.25623.1.0.111050)
Summary vsftpd is prone to a security-bypass vulnerability.
Vulnerability Detection Result Installed version: 2.3.4 Fixed version: 3.0.3
Impact An attacker can exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks.
Solution Solution type: VendorFix A fixed version 3.0.3 is available. Please see the references for more information.
Affected Software/OS vsftpd versions 3.0.2 and below are vulnerable.
Vulnerability Detection Method Details: vsftpd < 3.0.3 Security Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.108045 Version used: \$Revision: 5026 \$
... continues on next page ...

...continued from previous page ...

Product Detection Result

Product: cpe:/a:beasts:vsftpd:2.3.4
 Method: vsFTPD FTP Server Detection
 OID: 1.3.6.1.4.1.25623.1.0.111050)

References

CVE: CVE-2015-1419
 BID: 72451
 Other:
 URL: <http://www.securityfocus.com/bid/72451>
 URL: <https://security.appspot.com/vsftpd/Changelog.txt>
 URL: <https://security.appspot.com/vsftpd.html>

[\[return to 10.0.2.4 \]](#)**Medium 53/tcp**

Medium (CVSS: 4.3)

NVT: ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability

Product detection result

cpe:/a:isc:bind:9.4.2
 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)

Summary

The host is installed with ISC BIND and is prone to denial of service vulnerability.

Vulnerability Detection Result

Installed version: 9.4.2
 Fixed version: 9.9.9-P2

Impact

Successful exploitation will allow remote attackers to cause denial of service.

Solution

Solution type: VendorFix
 Upgrade to ISC BIND version 9.9.9-P2 or 9.10.4-P2 or 9.11.0b2 or later.

Affected Software/OS

ISC BIND versions 9.0.x through 9.9.9-P1, 9.10.0 through 9.10.4-P1, 9.11.0a3 through 9.11.0b1.

Vulnerability Insight

... continues on next page ...

...continued from previous page ...
The flaw is due to an error in the BIND implementation of the lightweight resolver protocol which use alternate method to do name resolution.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.808751 Version used: \$Revision: 12455 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2016-2775 BID:92037 Other: URL: https://kb.isc.org/article/AA-01393/74/CVE-2016-2775 URL: https://www.isc.org

Medium (CVSS: 4.3) NVT: ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
Summary ISC BIND is prone to a remote denial-of-service vulnerability because the application fails to properly handle specially crafted dynamic update requests.
Vulnerability Detection Result The scanner only checked the version number (from TXT record in the Chaos class) because "safe checks" are enabled.
Impact Successfully exploiting this issue allows remote attackers to crash affected DNS servers, denying further service to legitimate users.
Solution Solution type: VendorFix
... continues on next page ...

...continued from previous page ...
The vendor released an advisory and fixes to address this issue. Please see the references for more information.
Affected Software/OS Versions prior to BIND 9.4.3-P3, 9.5.1-P3, and 9.6.1-P1 are vulnerable.
Vulnerability Detection Method Details: ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.100251 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2009-0696 BID:35848 Other: URL:http://www.securityfocus.com/bid/35848 URL:https://bugzilla.redhat.com/show_bug.cgi?id=514292 URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=538975 URL:http://www.isc.org/products/BIND/ URL:https://www.isc.org/node/474 URL:http://www.kb.cert.org/vuls/id/725188
Medium (CVSS: 4.0) NVT: ISC BIND AXFR Response Denial of Service Vulnerability
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
Summary ISC BIND is prone to a denial of service vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: Workaround
Impact An authenticated remote attacker may cause a denial of service condition.
... continues on next page ...

...continued from previous page ...

Solution**Solution type:** Workaround

As a workaround operators of servers which accept untrusted zone data can mitigate their risk by operating an intermediary server whose role it is to receive zone data and then (if successful) re-distribute it to client-facing servers. Successful exploitation of the attack against the intermediary server may still occur but denial of service against the client-facing servers is significantly more difficult to achieve in this scenario.

Affected Software/OS

Version \leq 9.10.4-P1

Vulnerability Insight

Primary DNS servers may cause a denial of service (secondary DNS server crash) via a large AXFR response, and possibly allows IXFR servers to cause a denial of service (IXFR client crash) via a large IXFR response and allows remote authenticated users to cause a denial of service (primary DNS server crash) via a large UPDATE message

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: ISC BIND AXFR Response Denial of Service Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.106118

Version used: \$Revision: 12096 \$

Product Detection Result

Product: cpe:/a:isc:bind:9.4.2

Method: Determine which version of BIND name daemon is running

OID: 1.3.6.1.4.1.25623.1.0.10028)

References

CVE: CVE-2016-6170

Other:

URL: <http://www.openwall.com/lists/oss-security/2016/07/06/3>

URL: <https://lists.dns-oarc.net/pipermail/dns-operations/2016-July/015058.html>

Medium (CVSS: 5.0)

NVT: ISC BIND Denial of Service Vulnerability

Product detection result

cpe:/a:isc:bind:9.4.2

Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)

Summary

... continues on next page ...

...continued from previous page ...
ISC BIND is prone to a denial of service vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.9.9-P4
Impact An remote attacker may cause a denial of service condition.
Solution Solution type: VendorFix Upgrade to 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, 9.11.0-P1 or later.
Affected Software/OS BIND 9
Vulnerability Insight A defect in BIND's handling of responses containing a DNAME answer can cause a resolver to exit after encountering an assertion failure in db.c or resolver.c
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.106366 Version used: \$Revision: 12313 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2016-8864 Other: URL: https://kb.isc.org/article/AA-01434
Medium (CVSS: 6.8) NVT: ISC BIND Denial of Service Vulnerability - 02 - Jan16
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1 ↪.4.1.25623.1.0.10028)
... continues on next page ...

...continued from previous page ...
Summary The host is installed with ISC BIND and is prone to remote denial of service vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.9.8-P3
Impact Successful exploitation will allow remote attackers to cause denial of service.
Solution Solution type: VendorFix Upgrade to ISC BIND version 9.9.8-P3 or 9.10.3-P3 or 9.9.8-S4 or later.
Affected Software/OS ISC BIND versions 9.3.0 through 9.8.8, 9.9.0 through 9.9.8-P2, 9.9.3-S1 through 9.9.8-S3, 9.10.0 through 9.10.3-P2.
Vulnerability Insight The flaw is due to an error in 'apl_42.c' script in ISC BIND.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND Denial of Service Vulnerability - 02 - Jan16 OID:1.3.6.1.4.1.25623.1.0.806996 Version used: \$Revision: 14181 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2015-8704 Other: URL: https://kb.isc.org/article/AA-01335
Medium (CVSS: 5.0) NVT: ISC BIND Denial of Service Vulnerability - 03 - Jan16
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
... continues on next page ...

...continued from previous page ...
Summary The host is installed with ISC BIND and is prone to remote denial of service vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.9.8-P2
Impact Successful exploitation will allow remote attackers to cause denial of service.
Solution Solution type: VendorFix Upgrade to ISC BIND version 9.9.8-P2 or 9.10.3-P2 or later.
Affected Software/OS ISC BIND versions 9.0.x through 9.9.8, 9.10.0 through 9.10.3.
Vulnerability Insight The flaw is due to an error in 'db.c' script in ISC BIND.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND Denial of Service Vulnerability - 03 - Jan16 OID:1.3.6.1.4.1.25623.1.0.806997 Version used: \$Revision: 11922 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2015-8000 BID:79349 Other: URL: https://kb.isc.org/article/AA-01317 URL: https://www.isc.org

Medium (CVSS: 4.3)
NVT: ISC BIND lwresd Denial of Service Vulnerability

Product detection result
cpe:/a:isc:bind:9.4.2
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
... continues on next page ...

↔.4.1.25623.1.0.10028)	...continued from previous page ...
Summary ISC BIND is prone to a denial of service vulnerability.	
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.9.9-P2	
Impact An remote attacker may cause a denial of service condition.	
Solution Solution type: VendorFix Upgrade to 9.9.9-P1, 9.10.4-P1, 9.11.0b1 or later.	
Affected Software/OS BIND 9	
Vulnerability Insight The lwresd component in BIND (which is not enabled by default) could crash while processing an overlong request name. This could lead to a denial of service.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND lwresd Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.106292 Version used: \$Revision: 12149 \$	
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)	
References CVE: CVE-2016-2775 Other: URL: https://kb.isc.org/article/AA-01393	
Medium (CVSS: 5.0) NVT: ISC BIND NSID Request Denial of Service Vulnerability (Linux)	
Product detection result cpe:/a:isc:bind:9.4.2	
... continues on next page ...	

...continued from previous page ...
Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
Summary The host is installed with ISC BIND and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.9.9-P3 or 9.10.4-P3 or 9.11.0
Impact Successful exploitation will allow remote attackers to cause a denial of service.
Solution Solution type: VendorFix Upgrade to ISC BIND version 9.9.9-P3 or 9.10.4-P3 or 9.11.0 or later on Linux.
Affected Software/OS ISC BIND versions 9.1.0 through 9.8.4-P2 and 9.9.0 through 9.9.2-P2 on Linux.
Vulnerability Insight The flaw exists due to mishandling of packets with malformed options. A remote attacker could use this flaw to make named exit unexpectedly with an assertion failure via a specially crafted DNS packet.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND NSID Request Denial of Service Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.809461 Version used: \$Revision: 12455 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2016-2848 BID:93814 Other: URL: https://kb.isc.org/article/AA-01433/74/CVE-2016-2848 URL: https://www.isc.org

Medium (CVSS: 5.0) NVT: ISC BIND Resolver Cache Vulnerability - Jan16
Product detection result cpe:/a:isc:bind:9.4.2 Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)
Summary The host is installed with ISC BIND and is prone to resolver cache vulnerability.
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: Workaround
Impact Successful exploitation will allow remote attackers to trigger continued resolvability of domain names that are no longer registered.
Solution Solution type: Workaround As a workaround it is recommended to clear the cache, which will remove cached bad records but is not an effective or practical preventative approach.
Affected Software/OS ISC BIND versions 9 through 9.8.1-P1.
Vulnerability Insight The flaw exists due to the resolver overwrites cached server names and TTL values in NS records during the processing of a response to an A record query.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: ISC BIND Resolver Cache Vulnerability - Jan16 OID:1.3.6.1.4.1.25623.1.0.807217 Version used: \$Revision: 11938 \$
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)
References CVE: CVE-2012-1033 BID:51898 Other:
... continues on next page ...

...continued from previous page ...

URL:<https://www.kb.cert.org/vuls/id/542123>
 URL:<https://www.isc.org>

Medium (CVSS: 5.0)

NVT: ISC BIND RTYPE ANY Query Denial of Service Vulnerability (Linux)

Product detection result

cpe:/a:isc:bind:9.4.2

Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1
 ↪.4.1.25623.1.0.10028)

Summary

The host is installed with ISC BIND and is prone to denial of service vulnerability.

Vulnerability Detection Result

Installed version: 9.4.2

Fixed version: 9.9.9-P5

Impact

Successful exploitation will allow remote attackers to cause a denial of service (assertion failure and daemon exit) via crafted data.

Solution**Solution type:** VendorFix

Upgrade to ISC BIND version 9.9.9-P5 or 9.10.4-P5 or 9.11.0-P2 or 9.9.9-S7 or later on Linux.

Affected Software/OS

ISC BIND versions 9.4.0 through 9.6-ESV-R11-W1, 9.8.5 through 9.8.8, 9.9.3 through 9.9.9-P4, 9.9.9-S1 through 9.9.9-S6, 9.10.0 through 9.10.4-P4 and 9.11.0 through 9.11.0-P1 on Linux.

Vulnerability Insight

The flaw exists due to an error in the processing of a malformed query response received in response to a RTYPE ANY query.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: ISC BIND RTYPE ANY Query Denial of Service Vulnerability (Linux)

OID:1.3.6.1.4.1.25623.1.0.810287

Version used: \$Revision: 11874 \$

Product Detection Result

Product: cpe:/a:isc:bind:9.4.2

Method: Determine which version of BIND name daemon is running

OID: 1.3.6.1.4.1.25623.1.0.10028)

... continues on next page ...

...continued from previous page ...

References

CVE: CVE-2016-9131

BID:95386

Other:

URL:<https://kb.isc.org/article/AA-01439/0>URL:<https://www.isc.org>

Medium (CVSS: 4.3)

NVT: ISC BIND Security Bypass Vulnerability

Product detection result

cpe:/a:isc:bind:9.4.2

Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)

Summary

A flaw was found in the way BIND handled TSIG authentication for dynamic updates. A remote attacker able to communicate with an authoritative BIND server could use this flaw to manipulate the contents of a zone, by forging a valid TSIG or SIG(0) signature for a dynamic update request.

Vulnerability Detection Result

Installed version: 9.4.2

Fixed version: 9.9.10-P2

Solution**Solution type:** VendorFix

Update to version 9.9.10-P2, 9.10.5-P2, 9.11.1-P2, 9.9.10-S3, 9.10.5-S3 or later.

Affected Software/OS

ISC BIND versions 9.4.0-9.8.8, 9.9.0-9.9.10-P1, 9.10.0-9.10.5-P1, 9.11.0-9.11.1-P1, 9.9.3-S1-9.9.10-S2 and 9.10.5-S1-9.10.5-S2

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: ISC BIND Security Bypass Vulnerability

OID:1.3.6.1.4.1.25623.1.0.106937

Version used: \$Revision: 13654 \$

Product Detection Result

Product: cpe:/a:isc:bind:9.4.2

Method: Determine which version of BIND name daemon is running

OID: 1.3.6.1.4.1.25623.1.0.10028)

... continues on next page ...

...continued from previous page ...

References

CVE: CVE-2017-3143

Other:

URL: <https://kb.isc.org/article/AA-01503/0>

Medium (CVSS: 6.8)

NVT: OpenSSL DSA_verify() Security Bypass Vulnerability in BIND

Product detection result

cpe:/a:isc:bind:9.4.2

Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)

Summary

The host is running BIND and is prone to Security Bypass Vulnerability.

Vulnerability Detection Result

Installed version: 9.4.2

Fixed version: 9.6.0 P1, 9.5.1 P1, 9.4.3 P1 or 9.3.6 P1

Impact

Successful exploitation could allow remote attackers to bypass the certificate validation checks and can cause man-in-the-middle attack via signature checks on DSA and ECDSA keys used with SSL/TLS.

Solution**Solution type:** VendorFix

Upgrade to version 9.6.0 P1, 9.5.1 P1, 9.4.3 P1, 9.3.6 P1.

Affected Software/OS

ISC BIND version prior to 9.2 or 9.6.0 P1 or 9.5.1 P1 or 9.4.3 P1 or 9.3.6 P1/Linux.

Vulnerability Insight

The flaw is due to improper validation of return value from OpenSSL's DSA_do_verify and VP_VerifyFinal functions.

Vulnerability Detection Method

Details: OpenSSL DSA_verify() Security Bypass Vulnerability in BIND

OID: 1.3.6.1.4.1.25623.1.0.800338

Version used: \$Revision: 14031 \$

Product Detection Result

Product: cpe:/a:isc:bind:9.4.2

Method: Determine which version of BIND name daemon is running

OID: 1.3.6.1.4.1.25623.1.0.10028)

... continues on next page ...

...continued from previous page ...

References

CVE: CVE-2008-5077, CVE-2009-0025, CVE-2009-0265

BID: 33150, 33151

Other:

URL: <https://www.isc.org/node/373>URL: <http://secunia.com/advisories/33404/>URL: <http://www.ocert.org/advisories/ocert-2008-016.html>[\[return to 10.0.2.4 \]](#)**Medium 22/tcp**

Medium (CVSS: 5.8)

NVT: OpenSSH 'child_set_env()' Function Security Bypass Vulnerability

Product detection result

cpe:/a:openbsd:openssh:4.7p1

Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary

OpenSSH is prone to a security-bypass vulnerability.

Vulnerability Detection Result

Installed version: 4.7p1

Fixed version: 6.6

Impact

The security bypass allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.

Solution**Solution type:** VendorFix

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

Checks if a vulnerable version is present on the target host.

Details: OpenSSH 'child_set_env()' Function Security Bypass Vulnerability

... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.105003 Version used: \$Revision: 14185 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 Method: SSH Server type and version OID: 1.3.6.1.4.1.25623.1.0.10267)
References CVE: CVE-2014-2532 BID:66355 Other: URL:http://www.securityfocus.com/bid/66355 URL:http://www.openssh.com

Medium (CVSS: 5.0) NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux)
Product detection result cpe:/a:openbsd:openssh:4.7p1 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.
Vulnerability Detection Result Installed version: 4.7p1 Fixed version: 7.6
Impact Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.
Solution Solution type: VendorFix Upgrade to OpenSSH version 7.6 or later.
Affected Software/OS OpenSSH versions before 7.6 on Linux
Vulnerability Insight The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.812051 Version used: \$Revision: 11983 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 Method: SSH Server type and version OID: 1.3.6.1.4.1.25623.1.0.10267)
References CVE: CVE-2017-15906 BID:101552 Other: URL: https://www.openssh.com/txt/release-7.6 URL: https://github.com/openbsd/src/commit/a6981567e8e URL: http://www.openssh.com

Medium (CVSS: 5.5) NVT: OpenSSH <= 7.2p1 - Xauth Injection
Product detection result cpe:/a:openbsd:openssh:4.7p1 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: 4.7p1 Fixed version: 7.2p2
Impact By injecting xauth commands one gains limited* read/write arbitrary files, information leakage or xauth-connect capabilities.
Solution Solution type: VendorFix Upgrade to OpenSSH version 7.2p2 or later.
Affected Software/OS OpenSSH versions before 7.2p2
... continues on next page ...

...continued from previous page ...
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 Checks if a vulnerable version is present on the target host. Details: OpenSSH <= 7.2p1 - Xauth Injection OID:1.3.6.1.4.1.25623.1.0.105581 Version used: \$Revision: 11811 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 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 URL: http://www.openssh.com

Medium (CVSS: 5.8) NVT: OpenSSH Certificate Validation Security Bypass Vulnerability
Product detection result cpe:/a:openbsd:openssh:4.7p1 Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
Summary OpenSSH is prone to a security-bypass vulnerability.
Vulnerability Detection Result Installed version: 4.7p1 Fixed version: See references
Impact Attackers can exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks.
Solution Solution type: VendorFix 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

Checks if a vulnerable version is present on the target host.

Details: OpenSSH Certificate Validation Security Bypass Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.105004

Version used: \$Revision: 12095 \$

Product Detection Result

Product: `cpe:/a:openbsd:openssh:4.7p1`

Method: SSH Server type and version

OID: 1.3.6.1.4.1.25623.1.0.10267)

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

Product detection result

`cpe:/a:openbsd:openssh:4.7p1`

Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary

OpenSSH is prone to a remote denial-of-service vulnerability.

Vulnerability Detection Result

Installed version: 4.7p1

Fixed version: See references

Impact

Exploiting this issue allows remote attackers to trigger denial-of- service conditions.

... continues on next page ...

...continued from previous page ...
Solution Solution type: VendorFix 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: 11213 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 Method: SSH Server type and version OID: 1.3.6.1.4.1.25623.1.0.10267)
References CVE: CVE-2010-5107 BID:58162 Other: URL:http://www.securityfocus.com/bid/58162 URL:http://www.openssh.com

Medium (CVSS: 5.0) NVT: OpenSSH Denial of Service Vulnerability - Jan16
Product detection result cpe:/a:openbsd:openssh:4.7p1 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: 4.7p1 Fixed version: 7.1p2
... continues on next page ...

...continued from previous page ...
Impact Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read and application crash).
Solution Solution type: VendorFix Upgrade to OpenSSH version 7.1p2 or later.
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 Checks if a vulnerable version is present on the target host. Details: OpenSSH Denial of Service Vulnerability - Jan16 OID:1.3.6.1.4.1.25623.1.0.806671 Version used: \$Revision: 12051 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 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:4.7p1 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: 4.7p1
... continues on next page ...

...continued from previous page ...	
Fixed version:	6.9
Impact Successful exploitation will allow remote attackers to bypass intended access restrictions.	
Solution Solution type: VendorFix Upgrade to OpenSSH version 6.9 or later.	
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 Checks if a vulnerable version is present on the target host. Details: OpenSSH Security Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.806049 Version used: \$Revision: 11872 \$	
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 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 URL:http://www.openssh.com	
Medium (CVSS: 5.0) NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Linux)	
Product detection result cpe:/a:openbsd:openssh:4.7p1 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 user enumeration vulnerability.	
Vulnerability Detection Result Installed version: 4.7p1	
... continues on next page ...	

...continued from previous page ...	
Fixed version:	7.8
Installation path / port:	22/tcp
Impact	Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.
Solution	Solution type: VendorFix Update to version 7.8 or later.
Affected Software/OS	OpenSSH versions 7.7 and prior on Linux
Vulnerability Insight	The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c
Vulnerability Detection Method	Checks if a vulnerable version is present on the target host. Details: OpenSSH User Enumeration Vulnerability-Aug18 (Linux) OID:1.3.6.1.4.1.25623.1.0.813864 Version used: \$Revision: 12956 \$
Product Detection Result	Product: cpe:/a:openbsd:openssh:4.7p1 Method: SSH Server type and version OID: 1.3.6.1.4.1.25623.1.0.10267)
References	CVE: CVE-2018-15473 Other: URL: http://www.openssh.com URL: https://0day.city/cve-2018-15473.html URL: https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0
Medium (CVSS: 4.3) NVT: SSH Weak Encryption Algorithms Supported	
Summary	The remote SSH server is configured to allow weak encryption algorithms.
... continues on next page ...	

...continued from previous page...

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

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: 13581 \$

References

Other:

... continues on next page ...

...continued from previous page ...

URL: <https://tools.ietf.org/html/rfc4253#section-6.3>URL: <https://www.kb.cert.org/vuls/id/958563>[\[return to 10.0.2.4 \]](#)**Medium 80/tcp**

Medium (CVSS: 5.0)

NVT: /doc directory browsable

Summary

The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

Vulnerability Detection ResultVulnerable url: <http://10.0.2.4/doc/>**Solution****Solution type:** Mitigation

Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:

```
<Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost
</Directory>
```

Vulnerability Detection Method

Details: /doc directory browsable

OID: 1.3.6.1.4.1.25623.1.0.10056

Version used: \$Revision: 14336 \$

References

CVE: CVE-1999-0678

BID: 318

Medium (CVSS: 4.9)

NVT: Apache 'Options' and 'AllowOverride' Directives Security Bypass Vulnerability

Product detection result

cpe:/a:apache:http_server:2.2.8

Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

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 ...
Vulnerability Detection Result Installed version: 2.2.8 Fixed version: 2.2.9
Impact 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.
Solution Solution type: VendorFix Update to version 2.2.9 or later.
Affected Software/OS Versions prior to Apache 2.2.9 are vulnerable.
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: 14031 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server Detection OID: 1.3.6.1.4.1.25623.1.0.900498)
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.
... continues on next page ...

...continued from previous page ...
Solution Solution type: VendorFix Upgrade to Apache HTTP Server version 2.2.22 or later.
Affected Software/OS Apache HTTP Server versions 2.2.0 through 2.2.21
Vulnerability Insight 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: 11857 \$
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 ↩1

Medium (CVSS: 6.4) NVT: Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux)
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
Summary This host is running Apache HTTP Server and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 2.2.8 Fixed version: 2.2.34
Impact Successful exploitation will allow remote attackers to cause the target service to crash. A remote user can obtain potentially sensitive information as well on the target system.
... continues on next page ...

...continued from previous page ...
Solution Solution type: VendorFix Upgrade to Apache HTTP Server 2.2.34 or 2.4.27 or later.
Affected Software/OS Apache HTTP Server 2.2.x before 2.2.34 and 2.4.x before 2.4.27 on Linux.
Vulnerability Insight The flaw exists due to error in Apache 'mod_auth_digest' which does not properly initialize memory used to process 'Digest' type HTTP Authorization headers.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux) OID:1.3.6.1.4.1.25623.1.0.811237 Version used: \$Revision: 14173 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server Detection OID: 1.3.6.1.4.1.25623.1.0.900498)
References CVE: CVE-2017-9788 BID:99569 Other: URL:http://www.securitytracker.com/id/1038906 URL:http://httpd.apache.org/security/vulnerabilities_22.html URL:http://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 5.0) NVT: Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
Summary This host is running Apache HTTP Server and is prone multiple vulnerabilities.
Vulnerability Detection Result Installed version: 2.2.8 Fixed version: 2.2.32
... continues on next page ...

...continued from previous page ...
Impact Successful exploitation will allow remote attackers to conduct request smuggling, response splitting and cache pollution attacks.
Solution Solution type: VendorFix Upgrade to Apache HTTP Server 2.2.32 or 2.4.25 or later.
Affected Software/OS Apache HTTP Server 2.2.x before 2.2.32 and 2.3.x through 2.4.24 prior to 2.4.25
Vulnerability Insight Multiple flaw exists as application accepted a broad pattern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and request header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitespace and remained in the request field member 'the_request', while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied additional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.812033 Version used: \$Revision: 11983 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server Detection OID: 1.3.6.1.4.1.25623.1.0.900498)
References CVE: CVE-2016-8743 BID:95077 Other: URL: https://httpd.apache.org/security/vulnerabilities_22.html URL: https://httpd.apache.org/security/vulnerabilities_24.html
Medium (CVSS: 5.1) NVT: Apache HTTP Server Man-in-the-Middle attack Vulnerability - July16 (Linux)
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
... continues on next page ...

...continued from previous page ...
Summary This host is installed with Apache HTTP Server and is prone to man-in-the-middle attack vulnerability.
Vulnerability Detection Result Installed version: 2.2.8 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.
Solution Solution type: VendorFix Upgrade to version 2.4.24, or 2.2.32, or newer.
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 Checks if a vulnerable version is present on the target host. 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: 12051 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server 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 URL: http://www.apache.org

Medium (CVSS: 5.0) NVT: Apache HTTP Server Mod_Lua Denial of service Vulnerability -01 May15
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
Summary This host is installed with Apache HTTP Server and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 2.2.8 Fixed version: 2.4.13
Impact Successful exploitation will allow a remote attackers to cause a denial of service via some crafted dimension.
Solution Solution type: VendorFix Upgrade to version 2.4.13 or later.
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 Checks if a vulnerable version is present on the target host. 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: 11975 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server 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
... continues on next page ...

...continued from previous page...

URL: <http://www.apache.org>

Medium (CVSS: 5.0)

NVT: Apache HTTP Server Multiple Remote Denial of Service Vulnerabilities

Product detection result

cpe:/a:apache:http_server:2.2.8

Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

Summary

Apache HTTP Server is prone to multiple remote denial-of-service vulnerabilities.

Vulnerability Detection Result

Installed version: 2.2.8

Fixed version: 2.2.16

Impact

An attacker can exploit these issues to deny service to legitimate users.

Solution**Solution type:** VendorFix

These issues have been fixed in Apache 2.2.16. Please see the references for more information.

Affected Software/OS

Versions prior to Apache 2.2.16 are vulnerable.

Vulnerability Detection Method

Details: Apache HTTP Server Multiple Remote Denial of Service Vulnerabilities

OID: 1.3.6.1.4.1.25623.1.0.100725

Version used: \$Revision: 13960 \$

Product Detection Result

Product: cpe:/a:apache:http_server:2.2.8

Method: Apache Web Server Detection

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

CVE: CVE-2010-1452

BID: 41963

Other:

URL: <https://www.securityfocus.com/bid/41963>URL: <http://httpd.apache.org/download.cgi>URL: <http://httpd.apache.org/>URL: <http://www.apache.org/dist/httpd/Announcement2.2.html>URL: http://www.apache.org/dist/httpd/CHANGES_2.2.16

Medium (CVSS: 5.0) NVT: Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed)
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
Summary Apache HTTP server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed.
Vulnerability Detection Result Installed version: 2.2.8 Fixed version: Apply the referenced patch or upgrade to 2.4.28
Impact The successful exploitation allows the attacker to read chunks of the host's memory.
Solution Solution type: VendorFix Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled competely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all <Limit> statements within the webserver configuration needs to be verified for invalid HTTP methods.
Affected Software/OS Apache HTTP Server 2.2.x versions up to 2.2.34 and 2.4.x below 2.4.28.
Vulnerability Insight Optionsbleed is a use after free error in Apache HTTP server that causes a corrupted Allow header to be constructed in response to HTTP OPTIONS requests. This can leak pieces of arbitrary memory from the server process that may contain secrets. The memory pieces change after multiple requests, so for a vulnerable host an arbitrary number of memory chunks can be leaked. The bug appears if a webmaster tries to use the 'Limit' directive with an invalid HTTP method. Example .htaccess: <Limit abcxzy> </Limit>
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) OID:1.3.6.1.4.1.25623.1.0.108252 Version used: \$Revision: 11983 \$
Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server Detection OID: 1.3.6.1.4.1.25623.1.0.900498)
References CVE: CVE-2017-9798 BID: 100872 Other: URL: http://openwall.com/lists/oss-security/2017/09/18/2 URL: https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-leak-Apaches-server-memory.html URL: http://www.securityfocus.com/bid/100872 URL: https://archive.apache.org/dist/httpd/patches/apply_to_2.2.34/ URL: https://www.apache.org/dist/httpd/CHANGES_2.4.28

Medium (CVSS: 5.0) NVT: Apache mod_proxy_ajp Information Disclosure Vulnerability
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
Summary This host is running Apache Web Server and is prone to Information Disclosure Vulnerability.
Vulnerability Detection Result Installed version: 2.2.8 Fixed version: 2.2.15
Impact Successful exploitation will let the attacker craft a special HTTP POST request and gain sensitive information about the web server.
Solution Solution type: VendorFix Upgrade to Apache HTTP Version 2.2.15 or later For further updates Workaround: Update mod_proxy_ajp.c through SVN Repository (Revision 767089), see the references for a patch file containing an update.
Affected Software/OS Apache HTTP Versions prior to 2.2.15 running mod_proxy_ajp.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
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: 14031 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server Detection OID: 1.3.6.1.4.1.25623.1.0.900498)
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 URL:https://archive.apache.org/dist/httpd/patches/apply_to_2.2.11/PR46949.diff ↪f URL:http://httpd.apache.org/download.cgi

Medium (CVSS: 4.3)
NVT: Apache mod_proxy_ftp Wildcard Characters XSS Vulnerability
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
Summary The host is running Apache, which is prone to cross-site scripting vulnerability.
Vulnerability Detection Result Installed version: 2.2.8 Fixed version: See references
Impact Remote attackers can execute arbitrary script code.
Solution Solution type: VendorFix
... continues on next page ...

...continued from previous page ...
Fixed is available in the SVN repository, please see the references for more information.
Affected Software/OS Apache 2.0.0 to 2.0.63 and Apache 2.2.0 to 2.2.9.
Vulnerability Insight Input passed to the module mod_proxy_ftp with wildcard character is not properly sanitized before returning to the user.
Vulnerability Detection Method Details: Apache mod_proxy_ftp Wildcard Characters XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.900107 Version used: \$Revision: 14010 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server Detection OID: 1.3.6.1.4.1.25623.1.0.900498)
References CVE: CVE-2008-2939 BID:30560 Other: URL:http://httpd.apache.org/ URL:http://www.securityfocus.com/archive/1/495180 URL:http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html URL:http://svn.apache.org/viewvc?view=rev&revision=682871 URL:http://svn.apache.org/viewvc?view=rev&revision=682868
Medium (CVSS: 5.0) NVT: awiki Multiple Local File Include Vulnerabilities
Summary awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.
Vulnerability Detection Result Vulnerable url: http://10.0.2.4/mutillidae/index.php?page=/etc/passwd
Impact An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host. Other attacks are also possible.
Solution ... continues on next page ...

...continued from previous page ...
Solution type: WillNotFix No known solution was made available for at least one year since the 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 awiki 20100125 is vulnerable. Other versions may also be affected.
Vulnerability Detection Method Details: awiki Multiple Local File Include Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.103210 Version used: \$Revision: 10741 \$
References BID:49187 Other: URL:https://www.exploit-db.com/exploits/36047/ URL:http://www.securityfocus.com/bid/49187 URL:http://www.kobaonline.com/awiki/
Medium (CVSS: 4.8) NVT: Cleartext Transmission of Sensitive Information via HTTP
Summary The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
Vulnerability Detection Result The following input fields where identified (URL:input name): http://10.0.2.4/phpMyAdmin/:pma_password http://10.0.2.4/phpMyAdmin/?D=A:pma_password http://10.0.2.4/tikiwiki/tiki-install.php:pass
Impact An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
Solution Solution type: Workaround Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.
<p>Vulnerability Detection Method</p> <p>Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.</p> <p>The script is currently checking the following:</p> <ul style="list-style-type: none"> - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password' <p>Details: Cleartext Transmission of Sensitive Information via HTTP</p> <p>OID:1.3.6.1.4.1.25623.1.0.108440</p> <p>Version used: \$Revision: 10726 \$</p>
<p>References</p> <p>Other:</p> <p>URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</p> <p>URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</p> <p>URL:https://cwe.mitre.org/data/definitions/319.html</p>

Medium (CVSS: 5.0)
NVT: Enabled Directory Listing Detection
<p>Summary</p> <p>The script attempts to identify directories with an enabled directory listing.</p>
<p>Vulnerability Detection Result</p> <p>The following directories with an enabled directory listing were identified:</p> <p>http://10.0.2.4/dav</p> <p>http://10.0.2.4/doc</p> <p>http://10.0.2.4/mutillidae/documentation</p> <p>http://10.0.2.4/test</p> <p>http://10.0.2.4/test/testoutput</p> <p>Please review the content manually.</p>
<p>Impact</p> <p>Based on the information shown an attacker might be able to gather additional info about the structure of this application.</p>
<p>Solution</p> <p>Solution type: Mitigation</p> <p>If not needed disable the directory listing within the webservers config.</p>
<p>Affected Software/OS</p> <p>Webservers with an enabled directory listing.</p>
... continues on next page ...

...continued from previous page ...

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: 5.8)

NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary

Debugging functions are enabled on the remote web server.

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result

The web server has the following HTTP methods enabled: TRACE

Impact

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution

Solution type: Mitigation

Disable the TRACE and TRACK methods in your web server configuration.

Please see the manual of your web server or the references for more information.

Affected Software/OS

Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight

It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method

Details: HTTP Debugging Methods (TRACE/TRACK) Enabled

OID:1.3.6.1.4.1.25623.1.0.11213

Version used: \$Revision: 10828 \$

References

CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683, CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE

... continues on next page ...

...continued from previous page ...
↔-2014-7883 BID:9506, 9561, 11604, 15222, 19915, 24456, 33374, 36956, 36990, 37995 Other: URL:http://www.kb.cert.org/vuls/id/288308 URL:http://www.kb.cert.org/vuls/id/867593 URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable URL:https://www.owasp.org/index.php/Cross_Site_Tracing

Medium (CVSS: 5.0) NVT: PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to a Denial of Service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.39 Installation path / port: 80/tcp
Impact Successful exploitation will allow attackers to cause a denial of service of the affected application.
Solution Solution type: VendorFix Update to version 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 or later.
Affected Software/OS PHP versions 5.x before 5.6.39, 7.0.x before 7.0.33, 7.1.x before 7.1.26 and 7.2.x before 7.2.14.
Vulnerability Insight The flaw exist due to a NULL pointer dereference and application crash via an empty string in the message argument to the imap_mail function of ext/imap/php_imap.c.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.108505 Version used: \$Revision: 12938 \$
Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2018-19935 BID: 106143 Other: URL: https://bugs.php.net/bug.php?id=77020 URL: http://www.securityfocus.com/bid/106143

Medium (CVSS: 4.3) NVT: PHP 'exif_read_data()' JPEG Image Processing Denial Of Service Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to a denial-of-service vulnerability in its exif_read_data()' function.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.10
Impact Successful exploits may allow remote attackers to cause denial-of- service conditions in applications that use the vulnerable function.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS Versions prior to PHP 5.2.10 are affected.
Vulnerability Detection Method Details: PHP 'exif_read_data()' JPEG Image Processing Denial Of Service Vulnerability OID: 1.3.6.1.4.1.25623.1.0.100581 Version used: \$Revision: 10459 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote)
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2009-2687 BID: 35440 Other: URL: http://www.securityfocus.com/bid/35440 URL: http://www.php.net/releases/5_2_10.php URL: http://www.php.net/ URL: http://lists.debian.org/debian-security-announce/2009/msg00263.html URL: http://archives.neohapsis.com/archives/fulldisclosure/2009-08/0339.html URL: http://support.avaya.com/css/P8/documents/100072880

Medium (CVSS: 5.0) NVT: PHP 'ext/imap/php_imap.c' Use After Free Denial of Service Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is running PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.15/5.3.4
Impact Successful exploitation could allow local attackers to crash the affected application, denying service to legitimate users.
Solution Solution type: VendorFix Upgrade to PHP 5.2.15 or 5.3.4
Affected Software/OS PHP version 5.2 before 5.2.15 and 5.3 before 5.3.4
Vulnerability Insight The flaw is due to an error in 'imap_do_open' function in the IMAP extension 'ext/imap/php_imap.c'.
Vulnerability Detection Method Details: PHP 'ext/imap/php_imap.c' Use After Free Denial of Service Vulnerability ... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.801583 Version used: \$Revision: 11997 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2010-4150 BID:44980 Other: URL:http://xforce.iss.net/xforce/xfdb/63390 URL:http://svn.php.net/viewvc?view=revision&revision=305032 URL:http://www.php.net/downloads.php

Medium (CVSS: 5.0) NVT: PHP 'extract()' Function Security Bypass Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is running PHP and is prone to security bypass vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.2.15 or later
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.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Details: PHP 'extract()' Function Security Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.801731 Version used: \$Revision: 11987 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 URL:http://www.php.net/downloads.php

Medium (CVSS: 4.3) NVT: PHP 'filter_var()' function Stack Consumption Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is running PHP and is prone to a stack consumption vulnerability
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.15/5.3.4
Impact Successful exploitation could allow remote attackers to cause a denial of service (memory consumption and application crash) via a long e-mail address string.
Solution Solution type: VendorFix Upgrade to PHP version 5.2.15/5.3.4 or later.
Affected Software/OS PHP version 5.2 through 5.2.14 and 5.3 through 5.3.3
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - The flaw exists due to an error in 'filter_var()' function, when FILTER_VALIDATE_EMAIL mode is used while processing the long e-mail address string. - A NULL pointer dereference vulnerability exists in 'ZipArchive::getArchiveComment'.
Vulnerability Detection Method Details: PHP 'filter_var()' function Stack Consumption Vulnerability OID:1.3.6.1.4.1.25623.1.0.801547 Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2010-3710, CVE-2010-3709 Other: URL:http://bugs.php.net/bug.php?id=52929 URL:https://bugzilla.redhat.com/show_bug.cgi?id=646684 URL:http://www.securityfocus.com/archive/1/514562/30/150/threaded URL:http://www.php.net/downloads.php

Medium (CVSS: 5.0) NVT: PHP 'imageRotate()' Memory Information Disclosure Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The host is running PHP and is prone to Memory Information Disclosure vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.9
Impact Successful exploitation could let the attacker read the contents of arbitrary memory locations through a crafted value for an indexed image.
Solution Solution type: VendorFix Upgrade to PHP version 5.2.9 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS PHP version 5.x to 5.2.8 on all running platform.
Vulnerability Insight The flaw is due to improper validation of bgd_color or clrBack argument in imageRotate function.
Vulnerability Detection Method Details: PHP 'imageRotate()' Memory Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.900186 Version used: \$Revision: 14010 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2008-5498 BID:33002 Other: URL: http://securitytracker.com/alerts/2008/Dec/1021494.html URL: http://downloads.securityfocus.com/vulnerabilities/exploits/33002.php URL: http://downloads.securityfocus.com/vulnerabilities/exploits/33002-2.php

Medium (CVSS: 4.3) NVT: PHP 'LibGD' Denial of Service Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.4.32/5.5.16/5.6.0
Impact Successful exploitation will allow remote attackers to conduct denial of service attacks.
Solution Solution type: VendorFix Upgrade to PHP version 5.4.32 or 5.5.16 or 5.6.0 or later.
... continues on next page ...

...continued from previous page ...
Affected Software/OS PHP version 5.x through 5.4.26 and probably other versions.
Vulnerability Insight The flaw is due to a NULL pointer dereference error in 'gdImageCreateFromXpm' function within LibGD.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'LibGD' Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.804292 Version used: \$Revision: 11867 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2014-2497 BID:66233 Other: URL:https://bugs.php.net/bug.php?id=66901 URL:http://php.net

Medium (CVSS: 6.4) NVT: PHP 'make_http_soap_request' Information Disclosure Vulnerability (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service or information disclosure vulnerabilities
Vulnerability Detection Result Installed version: 5.2.4 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.
... continues on next page ...

...continued from previous page ...
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.
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 Checks if a vulnerable version is present on the target host. Details: PHP 'make_http_soap_request' Information Disclosure Vulnerability (Linux) OID: 1.3.6.1.4.1.25623.1.0.808666 Version used: \$Revision: 12051 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 'mb_strcut()' Function Information Disclosure Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to an information-disclosure vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.3.4
... continues on next page ...

...continued from previous page ...
Impact Attackers can exploit this issue to obtain sensitive information that may lead to further attacks.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS Versions prior to PHP 5.3.4 are vulnerable.
Vulnerability Detection Method Details: PHP 'mb_strcut()' Function Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.100898 Version used: \$Revision: 10459 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2010-4156 BID:44727 Other: URL: https://www.securityfocus.com/bid/44727 URL: http://permalink.gmane.org/gmane.comp.security.oss.general/3715 URL: http://www.php.net/

Medium (CVSS: 5.0) NVT: PHP 'open_basedir' Security Bypass Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to security bypass vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: N/A
Impact Successful exploitation will allow remote attackers to read arbitrary files.
... continues on next page ...

...continued from previous page ...
Solution Solution type: WillNotFix No known solution was made available for at least one year since the 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 versions 5.x.0 to 5.0.5, 5.1.0 to 5.1.6, 5.2.0 to 5.2.17, 5.3.0 to 5.3.27, 5.4.0 to 5.4.23 and 5.5.0 to 5.5.6.
Vulnerability Insight The flaw is in libxml RSHUTDOWN function which allows to bypass open_basedir protection mechanism through stream_close method call.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'open_basedir' Security Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.804241 Version used: \$Revision: 11867 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2012-1171 Other: URL: https://bugzilla.redhat.com/show_bug.cgi?id=802591

Medium (CVSS: 4.3) NVT: PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to cross site scripting and denial of service vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.33
...continues on next page ...

...continued from previous page...	
Installation	
path / port:	80/tcp
Impact	Successfully exploiting this issue allows attacker 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 and to launch other attacks and will also lead to a denial of service and exhausting the server resources.
Solution	
Solution type:	VendorFix
	Upgrade to PHP version 5.6.33, 7.0.27, 7.1.13 or 7.2.1 or later.
Affected Software/OS	
	PHP versions before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1
Vulnerability Insight	
	Multiple flaws are due to, - An input validation error on the PHAR 404 error page via the URI of a request for a .phar file. - An integer signedness error in gd_gif_in.c in the GD Graphics Library (aka libgd).
Vulnerability Detection Method	
	Checks if a vulnerable version is present on the target host. Details: PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Linux) OID:1.3.6.1.4.1.25623.1.0.812735 Version used: \$Revision: 12120 \$
Product Detection Result	
	Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References	
	CVE: CVE-2018-5712, CVE-2018-5711 Other: URL:http://php.net/ChangeLog-5.php URL:http://php.net/ChangeLog-7.php URL:https://bugs.php.net/bug.php?id=74782 URL:https://bugs.php.net/bug.php?id=75571 URL:http://www.php.net
Medium (CVSS: 6.4)	
NVT: PHP 'phar_parse_pharfile' Function Denial of Service Vulnerability - (Linux)	
Product detection result	
cpe:/a:php:php:5.2.4	
... continues on next page ...	

...continued from previous page ...
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.30
Impact Successfully exploiting this issue allow remote attackers to supply malicious archive files to crash the PHP interpreter or potentially disclose information.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.30 or 7.0.15, or later.
Affected Software/OS PHP versions before 5.6.30, 7.x before 7.0.15
Vulnerability Insight The flaw exists due to a buffer over-read error in the 'phar_parse_pharfile' function in ext/phar/phar.c script.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'phar_parse_pharfile' Function Denial of Service Vulnerability - (Linux) OID:1.3.6.1.4.1.25623.1.0.811484 Version used: \$Revision: 11863 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109
References CVE: CVE-2017-11147 Other: URL: http://www.php.net/ChangeLog-5.php URL: http://www.php.net/ChangeLog-7.php
Medium (CVSS: 6.8) NVT: PHP 'PHP-FPM' Denial of Service Vulnerability (Linux)
... continues on next page ...

...continued from previous page ...
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 7.1.20 Installation path / port: 80/tcp
Impact Successfully exploitation will allow an attackers to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.
Solution Solution type: VendorFix Update to PHP 7.1.20, 7.2.8 or 7.3.0alpha3.
Affected Software/OS PHP versions 5.x up to and including 5.6.36. All 7.0.x versions, 7.1.x before 7.1.20, 7.2.x before 7.2.8 and 7.3.x before 7.3.0alpha3 on Windows.
Vulnerability Insight The flaw exist due to the php-fpm master process restarts a child process in an endless loop when using program execution functions with a non-blocking STDIN stream.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'PHP-FPM' Denial of Service Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.812520 Version used: \$Revision: 12762 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2015-9253 Other: URL: https://bugs.php.net/bug.php?id=73342
... continues on next page ...

<p>...continued from previous page ...</p> <p>URL: https://bugs.php.net/bug.php?id=70185 URL: https://github.com/php/php-src/pull/3287 URL: https://www.futureweb.at/security/CVE-2015-9253 URL: https://vuldb.com/?id.113566</p>
<p>Medium (CVSS: 5.0) NVT: PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Linux)</p> <p>Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p> <p>Summary This host is installed with PHP and is prone to privilege escalation vulnerability.</p> <p>Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.5.32 Installation path / port: 80/tcp</p> <p>Impact Successfully exploitation will allow an attacker to update the 'metadata' and affect on confidentiality, integrity, and availability.</p> <p>Solution Solution type: VendorFix Upgrade to PHP version 5.5.32, 7.0.3, or 5.6.18 or later.</p> <p>Affected Software/OS PHP versions before 5.5.32, 7.0.x before 7.0.3, and 5.6.x before 5.6.18 on Linux.</p> <p>Vulnerability Insight The flaw exists due to error in the function stream_get_meta_data of the component File Upload. The manipulation as part of a Return Value leads to a privilege escalation vulnerability (Metadata).</p> <p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.812512 Version used: \$Revision: 12120 \$</p> <p>Product Detection Result Product: cpe:/a:php:php:5.2.4 ... continues on next page ...</p>

...continued from previous page ...
Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2016-10712 Other: URL: https://vuldb.com/?id.113055 URL: https://bugs.php.net/bug.php?id=71323 URL: https://git.php.net/?p=php-src.git;a=commit;h=6297a117d77fa3a0df2e21ca926↵a92c231819cd5 URL: http://www.php.net

Medium (CVSS: 5.0) NVT: PHP 'strchr()' Function Information Disclosure Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to an information-disclosure vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.3.3
Impact Attackers can exploit this issue to obtain sensitive information that may lead to further attacks.
Solution Solution type: VendorFix Updates are available. Please see the references for details.
Affected Software/OS PHP 5 through 5.3.2 are vulnerable.
Vulnerability Detection Method Details: PHP 'strchr()' Function Information Disclosure Vulnerability OID: 1.3.6.1.4.1.25623.1.0.100695 Version used: \$Revision: 10472 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote)
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2010-2484 BID: 41265 Other: URL: http://www.securityfocus.com/bid/41265 URL: http://permalink.gmane.org/gmane.comp.security.oss.general/3109 URL: http://www.php.net/

Medium (CVSS: 5.0) NVT: PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to heap buffer overflow vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.32 Installation path / port: 80/tcp
Impact Successfully exploiting this issue allow attacker to execute arbitrary code with elevated privileges within the context of a privileged process.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.32, 7.0.25, 7.1.11, or later.
Affected Software/OS PHP versions before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11
Vulnerability Insight The flaw exists due to an error in the date extension's 'timelib_meridian' handling of 'front of' and 'back of' directives.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Linux)
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.812073 Version used: \$Revision: 11983 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2017-16642 BID: 101745 Other: URL: http://php.net/ChangeLog-5.php URL: http://php.net/ChangeLog-7.php URL: https://bugs.php.net/bug.php?id=75055 URL: http://www.php.net

Medium (CVSS: 5.0) NVT: PHP 'unserialize()' Function Denial of Service Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The host is running PHP and is prone to Denial of Service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: None
Impact Successful exploitation could allow attackers to execute arbitrary PHP code and cause denial of service.
Solution Solution type: WillNotFix No known solution was made available for at least one year since the 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.
... continues on next page ...

...continued from previous page ...
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: 14031 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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.pdf ↪f

Medium (CVSS: 5.0) NVT: PHP 'URL checks' Security Bypass Vulnerability Jul17 (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to security bypass vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.28
Impact Successfully exploiting this issue allow an attacker to bypass hostname-specific URL checks.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.28, 7.0.13, or later.
Affected Software/OS PHP versions before 5.6.28, 7.x before 7.0.13
... continues on next page ...

...continued from previous page ...
Vulnerability Insight The flaw exists due to incorrect handling of various URI components in the URL parser.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'URL checks' Security Bypass Vulnerability Jul17 (Linux) OID:1.3.6.1.4.1.25623.1.0.811489 Version used: \$Revision: 11874 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2016-10397 Other: URL:http://www.php.net/ChangeLog-5.php URL:http://www.php.net/ChangeLog-7.php

Medium (CVSS: 5.0) NVT: PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.31
Impact Successfully exploiting this issue allow remote attackers inject XML for deserialization to crash the PHP interpreter.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.31 or later.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
PHP versions before 5.6.31.
Vulnerability Insight The flaw exists due to an invalid free error for an empty boolean element in ext/wddx/wddx.c script.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Linux) OID: 1.3.6.1.4.1.25623.1.0.811490 Version used: \$Revision: 11982 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2017-11143 Other: URL: http://www.php.net/ChangeLog-5.php

Medium (CVSS: 6.8) NVT: PHP 'xml_utf8_decode()' UTF-8 Input Validation Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to a vulnerability because it fails to sufficiently sanitize user-supplied input.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.3.4
Impact Exploiting this issue can allow attackers to provide unexpected input and possibly bypass input-validation protection mechanisms. This can aid in further attacks that may utilize crafted user-supplied input.
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 Versions prior to PHP 5.3.4 are vulnerable.
Vulnerability Detection Method Details: PHP 'xml_utf8_decode()' UTF-8 Input Validation Vulnerability OID:1.3.6.1.4.1.25623.1.0.100901 Version used: \$Revision: 10459 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2010-3870 BID:44605 Other: URL: https://www.securityfocus.com/bid/44605 URL: http://bugs.php.net/bug.php?id=48230 URL: http://bugs.php.net/bug.php?id=49687 URL: http://svn.php.net/viewvc?view=revision&revision=304959 URL: http://www.php.net/ URL: http://comments.gmane.org/gmane.comp.security.oss.general/3684 URL: http://www.mandriva.com/en/security/advisories?name=MDVSA-2010:224

Medium (CVSS: 5.0) NVT: PHP 'zend_strtod()' Function Floating-Point Value Denial of Service Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP is prone to a remote denial-of-service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.17/5.3.5
Impact Successful attacks will cause applications written in PHP to hang, creating a denial-of-service condition.
Solution
... continues on next page ...

...continued from previous page ...	
Solution type: VendorFix	Updates are available. Please see the references for more details.
Affected Software/OS	PHP 5.3.3 is vulnerable. Other versions may also be affected.
Vulnerability Insight	The vulnerability is due to the Floating-Point Value that exist in zend_strtod function
Vulnerability Detection Method	Details: PHP 'zend_strtod()' Function Floating-Point Value Denial of Service Vulnerability. ↪... OID:1.3.6.1.4.1.25623.1.0.103020 Version used: \$Revision: 10458 \$
Product Detection Result	Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References	CVE: CVE-2010-4645 BID:45668 Other: URL:https://www.securityfocus.com/bid/45668 URL:http://bugs.php.net/bug.php?id=53632 URL:http://svn.php.net/viewvc/?view=revision&revision=307119 URL:http://svn.php.net/viewvc?view=revision&revision=307095 URL:http://www.exploringbinary.com/php-hangs-on-numeric-value-2-2250738585072 ↪011e-308/ URL:http://www.php.net/
Medium (CVSS: 5.0) NVT: PHP 5.2.8 and Prior Versions Multiple Vulnerabilities	
Product detection result	cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary	PHP is prone to multiple security vulnerabilities.
Vulnerability Detection Result	Installed version: 5.2.4
... continues on next page ...	

...continued from previous page ...	
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.	
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: 14031 \$	
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References CVE: CVE-2009-1271 BID:33927 Other: URL:http://www.securityfocus.com/bid/33927 URL:http://www.php.net/	

Medium (CVSS: 5.0) NVT: PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14	
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)	
Summary This host is installed with PHP and is prone to denial of service vulnerabilities.	
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.4.29/5.5.13	
... continues on next page ...	

...continued from previous page ...
Impact Successful exploitation will allow remote attackers to conduct denial of service attacks.
Solution Solution type: VendorFix Upgrade to PHP version 5.4.29 or 5.5.13 or later.
Affected Software/OS PHP version 5.x before 5.4.29 and 5.5.x before 5.5.13
Vulnerability Insight The flaw is due to - An error due to an infinite loop within the 'unpack_summary_info' function in src/cdf.c script. - An error within the 'cdf_read_property_info' function in src/cdf.c script.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14 OID:1.3.6.1.4.1.25623.1.0.804639 Version used: \$Revision: 11867 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2014-0237, CVE-2014-0238 BID:67759, 67765 Other: URL:http://www.php.net/ChangeLog-5.php URL:http://secunia.com/advisories/58804 URL:https://www.hkcert.org/my_url/en/alert/14060401 URL:http://php.net
Medium (CVSS: 4.3) NVT: PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to cross-site scripting (XSS) vulnerability.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.4.38, or 5.5.22, or 5.6.6, or later.
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 Checks if a vulnerable version is present on the target host. Details: PHP Cross-Site Scripting Vulnerability - Aug16 (Linux) OID:1.3.6.1.4.1.25623.1.0.809137 Version used: \$Revision: 14181 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2015-8935 BID:92356 Other: URL: https://bugs.php.net/bug.php?id=68978
Medium (CVSS: 6.8) NVT: PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
... continues on next page ...

...continued from previous page ...
Summary This host is installed with PHP and is prone to denial of service and unspecified Vulnerabilities
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.18, or 7.0.3, or later.
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 Checks if a vulnerable version is present on the target host. 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: 12313 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 ... continues on next page ...

...continued from previous page ...
cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later.
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.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Denial of Service Vulnerability - 02 - Aug16 (Linux) OID:1.3.6.1.4.1.25623.1.0.809139 Version used: \$Revision: 12051 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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
... continues on next page ...

...continued from previous page ...
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The host is installed with PHP and is prone to Denial of Service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.9
Impact Successful exploitation could result in denial of service condition.
Solution Solution type: VendorFix Upgrade to version 5.2.9 or later.
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: 14031 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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
... continues on next page ...

...continued from previous page...	
Product detection result	cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary	PHP is prone to a denial-of-service vulnerability because the application fails to handle certain file requests.
Vulnerability Detection Result	Installed version: 5.2.4 Fixed version: 5.2.8
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.
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: 10459 \$
Product Detection Result	Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.0
Impact Successfully exploiting this issue allow remote attackers to cause a denial of service.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.0
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 Checks if a vulnerable version is present on the target host. Details: PHP Fileinfo Component Denial of Service Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.808669 Version used: \$Revision: 11961 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to Man-in-the-middle attack vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Update to PHP version 5.6.24 or 7.0.19.
Affected Software/OS PHP versions 5.x through 5.6.23 and 7.0.x through 7.0.8 on Linux
Vulnerability Insight The following flaws exist: - The web servers running in a CGI or CGI-like context may assign client request proxy header values to internal HTTP_PROXY environment variables. - 'HTTP_PROXY' is improperly trusted by some PHP libraries and applications - An unspecified flaw in the gdImageCropThreshold function in 'gd_crop.c' in the GD Graphics Library.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux) OID:1.3.6.1.4.1.25623.1.0.808628 Version used: \$Revision: 11969 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References ... continues on next page ...

...continued from previous page ...
<p>CVE: CVE-2016-5385, CVE-2016-6128</p> <p>BID: 91821, 91509</p> <p>Other:</p> <p>URL: http://www.php.net/ChangeLog-5.php</p> <p>URL: http://www.php.net/ChangeLog-7.php</p> <p>URL: http://www.kb.cert.org/vuls/id/797896</p> <p>URL: https://bugs.php.net/bug.php?id=72573</p> <p>URL: https://bugs.php.net/bug.php?id=72494</p>

<p>Medium (CVSS: 5.0)</p> <p>NVT: PHP Multiple Denial of Service Vulnerabilities (Linux)</p>
<p>Product detection result</p> <p>cpe:/a:php:php:5.2.4</p> <p>Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary</p> <p>This host is installed with PHP and is prone to multiple denial of service vulnerabilities.</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.2.4</p> <p>Fixed version: 5.6.12</p>
<p>Impact</p> <p>Successfully exploiting this issue allow remote attackers to cause a denial of service (application crash or memory consumption).</p>
<p>Solution</p> <p>Solution type: VendorFix</p> <p>Upgrade to PHP version 5.6.12 or later.</p>
<p>Affected Software/OS</p> <p>PHP versions prior to 5.6.12 on Linux</p>
<p>Vulnerability Insight</p> <p>Multiple flaws are due to</p> <ul style="list-style-type: none"> - 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.
<p>Vulnerability Detection Method</p> <p>Checks if a vulnerable version is present on the target host.</p> <p>Details: PHP Multiple Denial of Service Vulnerabilities (Linux)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.808611</p>
... continues on next page ...

...continued from previous page ...
Version used: \$Revision: 11961 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple denial of service vulnerabilities.
Vulnerability Detection Result Installed Version: 5.2.4 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).
Solution Solution type: VendorFix Upgrade to PHP 5.5.30 or 5.6.14 or later.
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 ... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host. Details: PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux) OID:1.3.6.1.4.1.25623.1.0.806649 Version used: \$Revision: 11872 \$</p>
<p>Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>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</p>

<p>Medium (CVSS: 5.0) NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Linux)</p>
<p>Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary This host is installed with PHP and is prone to multiple denial of service vulnerabilities.</p>
<p>Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.30</p>
<p>Impact Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer over-read or application crash).</p>
<p>Solution Solution type: VendorFix Upgrade to PHP version 5.6.30, 7.0.15, 7.1.1 or later.</p>
<p>Affected Software/OS PHP versions before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1.</p>
<p>Vulnerability Insight ... continues on next page ...</p>

...continued from previous page ...
<p>Multiple flaws are due to</p> <ul style="list-style-type: none"> - The <code>exif_convert_any_to_int</code> function in <code>ext/exif/exif.c</code> tries to divide the minimum representable negative integer by -1. - A mishandled serialized data in a <code>finish_nested_data</code> call within the <code>object_common1</code> function in <code>ext/standard/var_unserializer.c</code>.
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Multiple Denial of Service Vulnerabilities - 01 - Jan17 (Linux) OID: 1.3.6.1.4.1.25623.1.0.108052 Version used: \$Revision: 11863 \$</p>
<p>Product Detection Result Product: <code>cpe:/a:php:php:5.2.4</code> Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>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</p>
<p>Medium (CVSS: 4.3) NVT: PHP Multiple Heap Buffer Overflow Vulnerabilities (Linux)</p>
<p>Product detection result <code>cpe:/a:php:php:5.2.4</code> Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary This host is installed with PHP and is prone to denial of service vulnerability.</p>
<p>Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.37 Installation path / port: 80/tcp</p>
<p>Impact Successful exploitation will allow attackers to cause heap overflow and denial of service.</p>
<p>Solution Solution type: VendorFix</p>
... continues on next page ...

...continued from previous page ...
Upgrade to PHP version 5.6.37, 7.0.31, 7.1.20 or 7.2.8 or later. For updates refer to Reference links.
Affected Software/OS PHP versions before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8 on Linux.
Vulnerability Insight Multiple flaws exist due to, - 'exif_process_IFD_in_MAKERNOTE()' in exif.c file suffers from improper validation against crafted JPEG files. - 'exif_thumbnail_extract()' function in exif.c file suffers from improper validation of length of 'ImageInfo->Thumbnail.offset + ImageInfo->Thumbnail.size'
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Multiple Heap Buffer Overflow Vulnerabilities (Linux) OID:1.3.6.1.4.1.25623.1.0.813901 Version used: \$Revision: 12120 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2018-14851 Other: URL:http://www.php.net URL:https://bugs.php.net/bug.php?id=76557 URL:https://bugs.php.net/bug.php?id=76423
Medium (CVSS: 6.4) NVT: PHP Multiple Information Disclosure Vulnerabilities
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is running PHP and is prone to multiple information disclosure vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4
... continues on next page ...

...continued from previous page...	
Fixed version:	5.2.14/5.3.3
Impact Successful exploitation could allow local attackers to bypass certain security restrictions and to obtain sensitive information.	
Solution Solution type: VendorFix Upgrade to PHP version 5.2.14/5.3.3 or later	
Affected Software/OS PHP version 5.2 through 5.2.13 and 5.3 through 5.3.2	
Vulnerability Insight Multiple flaws are due to: - Error in 'trim()', 'ltrim()', 'rtrim()' and 'substr_replace()' functions, which causes a userspace interruption of an internal function within the call time pass by reference feature. - Error in 'parse_str()', 'preg_match()', 'unpack()' and 'pack()' functions, 'ZEND_FETCH_RW()', 'ZEND_CONCAT()', and 'ZEND_ASSIGN_CONCAT()' op-codes, and the 'ArrayObject::uasort' method, trigger memory corruption by causing a userspace interruption of an internal function or handler.	
Vulnerability Detection Method Details: PHP Multiple Information Disclosure Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.801359 Version used: \$Revision: 13960 \$	
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References CVE: CVE-2010-2190, CVE-2010-2191 Other: URL: http://www.php-security.org/2010/05/30/mops-2010-048-php-substr_replace-in-terruption-information-leak-vulnerability/index.html URL: http://www.php-security.org/2010/05/30/mops-2010-047-php-trimltrimrtrim-i-nterruption-information-leak-vulnerability/index.html URL: http://www.php.net/downloads.php	
Medium (CVSS: 5.0) NVT: PHP Multiple Security Bypass Vulnerabilities	
Product detection result cpe:/a:php:php:5.2.4	
... continues on next page ...	

...continued from previous page ...
Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is running PHP and is prone to multiple security bypass vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP 5.3.4 or later
Affected Software/OS PHP version prior to 5.3.4
Vulnerability Insight The flaws are caused to: <ul style="list-style-type: none"> - 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: 11987 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109
References CVE: CVE-2006-7243, CVE-2010-4699, CVE-2011-0754, CVE-2011-0753, CVE-2011-0755 Other: <ul style="list-style-type: none"> 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
... continues on next page ...

...continued from previous page ...
URL:http://svn.php.net/viewvc?view=revision&revision=305507 URL:http://www.php.net/downloads.php
Medium (CVSS: 5.0) NVT: PHP Multiple Vulnerabilities - Jul17 (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.31
Impact Successfully exploiting this issue allow remote attackers to leak information from the interpreter, crash PHP interpreter and also disclose sensitive information.
Solution Solution type: VendorFix Upgrade to PHP version 5.6.31, 7.0.21, 7.1.7, or later.
Affected Software/OS PHP versions before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7
Vulnerability Insight Multiple flaws are due to <ul style="list-style-type: none"> - An ext/date/lib/parse_date.c out-of-bounds read affecting the php_parse_date function. - The openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function. - lack of bounds checks in the date extension's timelib_meridian parsing code. - A stack-based buffer overflow in the zend_ini_do_op() function in 'Zend/zend_ini_parser.c' script. - The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd) does not zero colorMap arrays before use.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities - Jul17 (Linux) OID:1.3.6.1.4.1.25623.1.0.811482 Version used: \$Revision: 11900 \$
... continues on next page ...

...continued from previous page ...
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2017-11145, CVE-2017-11144, CVE-2017-11146, CVE-2017-11628, CVE-2017-78 ↪90 BID:99492, 99550, 99605, 99612, 99489 Other: URL:http://www.php.net/ChangeLog-5.php URL:http://www.php.net/ChangeLog-7.php

Medium (CVSS: 6.8) NVT: PHP Multiple Vulnerabilities May18 (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The host is installed with php and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.6.36 Installation path / port: 80/tcp
Impact Successful exploitation will allow an attacker to conduct XSS attacks, crash PHP, conduct denial-of-service condition and execute arbitrary code in the context of the affected application.
Solution Solution type: VendorFix Upgrade to version 7.2.5 or 7.0.30 or 5.6.36 or 7.1.17 or later. For updates refer to Reference links.
Affected Software/OS PHP versions prior to 5.6.36, PHP versions 7.2.x prior to 7.2.5, PHP versions 7.0.x prior to 7.0.30, PHP versions 7.1.x prior to 7.1.17 on Linux.
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
<p>Multiple flaws exists due to</p> <ul style="list-style-type: none"> - An out of bounds read error in 'exif_read_data' function while processing crafted JPG data. - An error in stream filter 'convert.iconv' which leads to infinite loop on invalid sequence. - An error in the LDAP module of PHP which allows a malicious LDAP server or man-in-the-middle attacker to crash PHP. - An error in the 'phar_do_404()' function in 'ext/phar/phar_object.c' script which returns parts of the request unfiltered, leading to another XSS vector. This is due to incomplete fix for CVE-2018-5712.
<p>Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Multiple Vulnerabilities May18 (Linux) OID:1.3.6.1.4.1.25623.1.0.813160 Version used: \$Revision: 12120 \$</p>
<p>Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References CVE: CVE-2018-10549, CVE-2018-10546, CVE-2018-10548, CVE-2018-10547 Other: URL:http://www.php.net/ChangeLog-5.php#5.6.36 URL:http://www.php.net/ChangeLog-7.php#7.0.30 URL:http://www.php.net/ChangeLog-7.php#7.1.17 URL:http://www.php.net/ChangeLog-7.php#7.2.5</p>
<p>Medium (CVSS: 6.4) NVT: PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)</p>
<p>Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary This host is installed with PHP and is prone to out-of-bounds read memory corruption vulnerability.</p>
<p>Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.5.31</p>
<p>Impact</p>
... continues on next page ...

...continued from previous page ...
Successfully exploiting this issue allow remote attackers to obtain sensitive information or cause a denial-of-service condition.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later.
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 Checks if a vulnerable version is present on the target host. 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: 12338 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 URL: http://www.php.net
Medium (CVSS: 4.3) NVT: PHP SOAP Parser Multiple Information Disclosure Vulnerabilities
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to multiple information disclosure vulnerabilities.
Vulnerability Detection Result ... continues on next page ...

...continued from previous page ...
Installed version: 5.2.4 Fixed version: 5.3.22/5.4.12
Impact Successful exploitation will allow remote attackers to obtain sensitive information.
Solution Solution type: VendorFix Upgrade to PHP 5.3.22 or 5.4.12 or later.
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 Checks if a vulnerable version is present on the target host. Details: PHP SOAP Parser Multiple Information Disclosure Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.803764 Version used: \$Revision: 11883 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2013-1824 BID:62373 Other: URL:http://php.net/ChangeLog-5.php URL:http://www.php.net/downloads.php URL:http://git.php.net/?p=php-src.git;a=commit;h=afe98b7829d50806559acac9b530 ↪acb8283c3bf4

Medium (CVSS: 6.8)

NVT: PHP Version 5.2 < 5.2.15 Multiple Vulnerabilities

Product detection result

cpe:/a:php:php:5.2.4

Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

... continues on next page ...

...continued from previous page ...
Summary PHP 5.2 < 5.2.15 suffers from multiple vulnerabilities such as a crash in the zip extract method, NULL pointer dereference and stack-based buffer overflow.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.15
Solution Solution type: VendorFix Upgrade to PHP version 5.2.15 or later.
Vulnerability Detection Method Details: PHP Version 5.2 < 5.2.15 Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.110066 Version used: \$Revision: 10460 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2010-3436, CVE-2010-3709, CVE-2010-4150, CVE-2010-4697, CVE-2010-4698, ↗CVE-2011-0752 BID:44718, 44723, 45335, 45952, 46448

Medium (CVSS: 5.0) NVT: PHP Version < 5.2.9 Multiple Vulnerabilities
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP version smaller than 5.2.9 suffers from multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.9
Solution Solution type: VendorFix Update PHP to version 5.2.9 or later.
... continues on next page ...

...continued from previous page ...
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: 10460 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary PHP version smaller than 5.3.4 suffers from multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.2.4 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: 10460 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References
... continues on next page ...

...continued from previous page ...
<p>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</p> <p>BID:40173, 43926, 44605, 44718, 44723, 44951, 44980, 45119, 45335, 45338, 45339, ↩ 45952, 45954, 46056, 46168</p>

<p>Medium (CVSS: 6.4)</p> <p>NVT: PHP Version < 5.3.9 Multiple Vulnerabilities</p>
<p>Product detection result</p> <p>cpe:/a:php:php:5.2.4</p> <p>Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary</p> <p>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.</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.2.4</p> <p>Fixed version: 5.3.9</p>
<p>Solution</p> <p>Solution type: VendorFix</p> <p>Upgrade PHP to 5.3.9 or versions after.</p>
<p>Vulnerability Detection Method</p> <p>Details: PHP Version < 5.3.9 Multiple Vulnerabilities</p> <p>OID:1.3.6.1.4.1.25623.1.0.110012</p> <p>Version used: \$Revision: 10460 \$</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:php:php:5.2.4</p> <p>Method: PHP Version Detection (Remote)</p> <p>OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References</p> <p>CVE: CVE-2011-4566, CVE-2011-4885, CVE-2012-0057, CVE-2012-0781, CVE-2012-0788, ↩CVE-2012-0789</p> <p>BID:50907, 51193, 51806, 51952, 51992, 52043</p>
... continues on next page ...

...continued from previous page ...

Medium (CVSS: 5.0)

NVT: PHP Versions Prior to 5.3.3/5.2.14 Multiple Vulnerabilities

Product detection result

cpe:/a:php:php:5.2.4

Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary

PHP is prone to multiple security vulnerabilities.

Vulnerability Detection Result

Installed version: 5.2.4

Fixed version: 5.2.14

Impact

An attacker can exploit these issues to execute arbitrary code, crash the affected application, gain access to sensitive information and bypass security restrictions. Other attacks are also possible.

Solution**Solution type:** VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

PHP 5.3 (Prior to 5.3.3) PHP 5.2 (Prior to 5.2.14)

Vulnerability Detection Method

Details: PHP Versions Prior to 5.3.3/5.2.14 Multiple Vulnerabilities

OID:1.3.6.1.4.1.25623.1.0.100726

Version used: \$Revision: 13960 \$

Product Detection Result

Product: cpe:/a:php:php:5.2.4

Method: PHP Version Detection (Remote)

OID: 1.3.6.1.4.1.25623.1.0.800109)

References

CVE: CVE-2010-2531, CVE-2010-2484

BID:41991

Other:

URL:https://www.securityfocus.com/bid/41991

URL:http://www.php.net/ChangeLog-5.php#5.3.3

URL:http://www.php.net/

Medium (CVSS: 6.8) NVT: PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary This host is installed with PHP and is prone to XML entity expansion and XML external entity vulnerabilities
Vulnerability Detection Result Installed version: 5.2.4 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.
Solution Solution type: VendorFix Upgrade to PHP version 5.5.22, or 5.6.6, or later.
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 Checks if a vulnerable version is present on the target host. 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: 12051 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
References CVE: CVE-2015-8866 BID:87470 Other: URL: http://www.php.net/ChangeLog-5.php

<p>Medium (CVSS: 6.8) NVT: PHP Zend and GD Multiple Denial of Service Vulnerabilities</p>
<p>Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>Summary This host is running PHP and is prone to multiple denial of service vulnerabilities.</p>
<p>Vulnerability Detection Result Installed version: 5.2.4 Fixed version: 5.2.15/5.3.5</p>
<p>Impact Successful exploitation could allow local attackers to crash the affected application, denying service to legitimate users.</p>
<p>Solution Solution type: VendorFix Upgrade to PHP 5.3.5 or later</p>
<p>Affected Software/OS PHP version prior to 5.2.15 and 5.3.x before 5.3.4</p>
<p>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.</p>
<p>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: 11997 \$</p>
<p>Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)</p>
<p>References CVE: CVE-2010-4697, CVE-2010-4698 Other: URL: http://bugs.php.net/52879 ... continues on next page ...</p>

...continued from previous page ...
URL:http://www.php.net/ChangeLog-5.php URL:http://www.php.net/downloads.php
Medium (CVSS: 4.3) NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 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.
Solution Solution type: WillNotFix No known solution was made available for at least one year since the 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.
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: 11553 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 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-2010-4480 Other: URL: http://www.exploit-db.com/exploits/15699/ URL: http://www.vupen.com/english/advisories/2010/3133
Medium (CVSS: 6.4) NVT: phpMyAdmin 3.x < 3.3.10.3; 3.4.x < 3.4.3.2 Multiple Vulnerabilities (Linux)
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary phpMyAdmin is prone to multiple vulnerabilities: - a Cross-Site Scripting (XSS) vulnerability in table Print view - possible superglobal and local variables manipulation in swekey authentication.
Vulnerability Detection Result Installed version: 3.1.1 Fixed version: 3.3.10.3
Solution Solution type: VendorFix Update to version 3.3.10.3, 3.4.3.2 or newer.
Affected Software/OS phpMyAdmin 3.x before 3.3.10.3 and 3.4.x before 3.4.3.2.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: phpMyAdmin 3.x < 3.3.10.3; 3.4.x < 3.4.3.2 Multiple Vulnerabilities (Linux) OID: 1.3.6.1.4.1.25623.1.0.108242 Version used: \$Revision: 12106 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References CVE: CVE-2011-2642, CVE-2011-2719 BID: 48874 Other: URL: https://www.phpmyadmin.net/security/PMASA-2011-9/
... continues on next page ...

...continued from previous page...

URL: <https://www.phpmyadmin.net/security/PMASA-2011-12/>

Medium (CVSS: 4.3)

NVT: phpMyAdmin <= 4.8.2 XSS Vulnerability - PMASA-2018-5 (Linux)

Product detection result

cpe:/a:phpmyadmin:phpmyadmin:3.1.1

Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary

phpMyAdmin is prone to an authenticated Cross-Site Scripting (XSS) Vulnerability.

Vulnerability Detection Result

Installed version: 3.1.1

Fixed version: 4.8.3

Solution**Solution type:** VendorFix

Update to version 4.8.3.

Affected Software/OS

phpMyAdmin through version 4.8.2.

Vulnerability Insight

An authenticated attacker could trick a user into importing a specially crafted file, resulting in the attacker gaining control over the user's account.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: phpMyAdmin <= 4.8.2 XSS Vulnerability - PMASA-2018-5 (Linux)

OID: 1.3.6.1.4.1.25623.1.0.113255

Version used: \$Revision: 12164 \$

Product Detection Result

Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1

Method: phpMyAdmin Detection

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

CVE: CVE-2018-15605

Other:

URL: <https://www.phpmyadmin.net/security/PMASA-2018-5/>

<p>Medium (CVSS: 6.5) NVT: phpMyAdmin Bookmark Security Bypass Vulnerability</p>
<p>Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p>Summary phpMyAdmin is prone to a security-bypass vulnerability that affects bookmarks.</p>
<p>Vulnerability Detection Result Installed version: 3.1.1 Fixed version: 3.3.9.2</p>
<p>Impact Successfully exploiting this issue allows a remote attacker to bypass certain security restrictions and perform unauthorized actions.</p>
<p>Solution Solution type: VendorFix Updates are available. Please see the references for details.</p>
<p>Affected Software/OS Versions prior to phpMyAdmin 3.3.9.2 and 2.11.11.3 are vulnerable.</p>
<p>Vulnerability Detection Method Details: phpMyAdmin Bookmark Security Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.103076 Version used: \$Revision: 11997 \$</p>
<p>Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p>References CVE: CVE-2011-0986, 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</p>
<p>... continues on next page ...</p>

...continued from previous page ...

Medium (CVSS: 4.3)

NVT: phpMyAdmin Cross-Site Scripting Vulnerability (PMASA-2018-3)-Linux

Product detection result

cpe:/a:phpmyadmin:phpmyadmin:3.1.1

Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary

This host is installed with phpMyAdmin and is prone to cross site scripting vulnerability.

Vulnerability Detection Result

Installed version: 3.1.1

Fixed version: 4.8.2

Installation

path / port: /phpMyAdmin

Impact

Successful exploitation will allow an attacker to inject arbitrary web script or HTML via crafted database name.

Solution**Solution type:** VendorFix

Upgrade to version 4.8.2 or newer. For updates refer to Reference links.

Affected Software/OS

phpMyAdmin versions prior to 4.8.2 on Linux

Vulnerability Insight

The flaw exists due to insufficient validation of input passed to 'js/designer/move.js' script in phpMyAdmin.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: phpMyAdmin Cross-Site Scripting Vulnerability (PMASA-2018-3)-Linux

OID:1.3.6.1.4.1.25623.1.0.813451

Version used: \$Revision: 12025 \$

Product Detection Result

Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1

Method: phpMyAdmin Detection

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

CVE: CVE-2018-12581

... continues on next page ...

...continued from previous page ...	
BID:104530	
Other:	
URL:https://www.phpmyadmin.net	
URL:https://www.phpmyadmin.net/security/PMASA-2018-3	
Medium (CVSS: 4.3)	
NVT: phpMyAdmin Database Search Cross Site Scripting Vulnerability	
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)	
Summary phpMyAdmin is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.	
Vulnerability Detection Result Installed version: 3.1.1 Fixed version: 2.11.11.1/3.3.8.1	
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 may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.	
Solution Solution type: VendorFix Vendor updates are available. Please see the references for more information.	
Affected Software/OS Versions prior to phpMyAdmin 3.3.8.1 and 2.11.11.1 are vulnerable.	
Vulnerability Detection Method Details: phpMyAdmin Database Search Cross Site Scripting Vulnerability OID:1.3.6.1.4.1.25623.1.0.100939 Version used: \$Revision: 13960 \$	
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)	
References CVE: CVE-2010-4329	
... continues on next page ...	

...continued from previous page ...
<p>BID:45100</p> <p>Other:</p> <p>URL:https://www.securityfocus.com/bid/45100</p> <p>URL:http://www.phpmyadmin.net/</p> <p>URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-8.php</p>
<p>Medium (CVSS: 4.3)</p> <p>NVT: phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability</p>
<p>Product detection result</p> <p>cpe:/a:phpmyadmin:phpmyadmin:3.1.1</p> <p>Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p>Summary</p> <p>phpMyAdmin is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 3.1.1</p> <p>Fixed version: 3.3.6</p>
<p>Impact</p> <p>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 and to launch other attacks.</p>
<p>Solution</p> <p>Solution type: VendorFix</p> <p>Vendor updates are available. Please see the references for more information.</p>
<p>Affected Software/OS</p> <p>Versions prior to phpMyAdmin 3.3.6 are vulnerable. Other versions may also be affected.</p>
<p>Vulnerability Detection Method</p> <p>Details: phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability</p> <p>OID:1.3.6.1.4.1.25623.1.0.100775</p> <p>Version used: \$Revision: 13960 \$</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1</p> <p>Method: phpMyAdmin Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p>References</p> <p>... continues on next page ...</p>

...continued from previous page ...
<p>CVE: CVE-2010-2958 BID: 42874 Other: URL: https://www.securityfocus.com/bid/42874 URL: http://www.phpmyadmin.net/ URL: http://www.phpmyadmin.net/home_page/security/PMASA-2010-6.php URL: http://www.phpmyadmin.git.sourceforge.net/git/gitweb.cgi?p=phpmyadmin/php↵myadmin;a=commitdiff;h=133a77fac7d31a38703db2099a90c1b49de62e37</p>

<p>Medium (CVSS: 4.3) NVT: phpMyAdmin Multiple Cross Site Scripting Vulnerabilities</p>
<p>Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p>Summary phpMyAdmin is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.</p>
<p>Vulnerability Detection Result Installed version: 3.1.1 Fixed version: 2.11.10.1/3.3.5.1</p>
<p>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 can allow the attacker to steal cookie-based authentication credentials and launch other attacks.</p>
<p>Solution Solution type: VendorFix Updates are available. Please see the references for details.</p>
<p>Affected Software/OS phpMyAdmin 2.11.x prior to 2.11.10.1 phpMyAdmin 3.x prior to 3.3.5.1</p>
<p>Vulnerability Detection Method Details: phpMyAdmin Multiple Cross Site Scripting Vulnerabilities OID: 1.3.6.1.4.1.25623.1.0.100761 Version used: \$Revision: 13960 \$</p>
<p>Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
... continues on next page ...

...continued from previous page ...
References CVE: CVE-2010-3056 BID: 42584 Other: URL: https://www.securityfocus.com/bid/42584 URL: http://www.phpmyadmin.net/ URL: http://www.phpmyadmin.net/home_page/security/PMASA-2010-5.php
Medium (CVSS: 4.3) NVT: phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 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 Installed version: 3.1.1 Fixed version: 3.3.7
Impact Successful exploitation will allow attackers to execute arbitrary web script or HTML in a user's browser session in the context of an affected site.
Solution Solution type: VendorFix Upgrade to phpMyAdmin version 3.3.7 or later.
Affected Software/OS phpMyAdmin versions 3.x before 3.3.7
Vulnerability Insight The flaw is caused by an unspecified input validation error when processing spoofed requests sent to setup script, which could be exploited by attackers to cause arbitrary scripting code to be executed on the user's browser session in the security context of an affected site.
Vulnerability Detection Method Details: phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability OID: 1.3.6.1.4.1.25623.1.0.801286 Version used: \$Revision: 13960 \$
Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References CVE: CVE-2010-3263 Other: URL: http://secunia.com/advisories/41210 URL: http://xforce.iss.net/xforce/xfdb/61675 URL: http://www.phpmyadmin.net/home_page/security/PMASA-2010-7.php URL: http://www.phpmyadmin.net/home_page/downloads.php

Medium (CVSS: 4.3) NVT: phpMyAdmin SQL bookmark XSS Vulnerability
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 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 Installed version: 3.1.1 Fixed version: 3.2.0.1
Impact Successful exploitation will let the attacker cause XSS attacks and inject malicious web script or HTML code via a crafted SQL bookmarks.
Solution Solution type: VendorFix Upgrade to phpMyAdmin version 3.2.0.1 or later.
Affected Software/OS phpMyAdmin version 3.0.x to 3.2.0.rc1.
Vulnerability Insight This flaw arises because the input passed into SQL bookmarks is not adequately sanitised before using it in dynamically generated content.
Vulnerability Detection Method Details: phpMyAdmin SQL bookmark XSS Vulnerability OID: 1.3.6.1.4.1.25623.1.0.800595
... continues on next page ...

...continued from previous page ...
Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References CVE: CVE-2009-2284 BID: 35543 Other: URL: http://secunia.com/advisories/35649 URL: http://www.phpmyadmin.net/home_page/security/PMASA-2009-5.php URL: http://www.phpmyadmin.net/home_page/downloads.php

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability
Product detection result cpe:/a:tikiwiki_cms/groupware:1.9.5 Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.↔0.901001)
Summary The host is installed with Tiki Wiki CMS Groupware and is prone to a local file inclusion vulnerability.
Vulnerability Detection Result Installed version: 1.9.5 Fixed version: 12.11
Impact Successful exploitation will allow an user having access to the admin backend to gain access to arbitrary files and to compromise the application.
Solution Solution type: VendorFix Upgrade to Tiki Wiki CMS Groupware version 12.11 LTS, 15.4 or later.
Affected Software/OS Tiki Wiki CMS Groupware versions: - below 12.11 LTS - 13.x, 14.x and 15.x below 15.4
... continues on next page ...

...continued from previous page ...
Vulnerability Insight The Flaw is due to improper sanitization of input passed to the 'fixedURLData' parameter of the 'display_banner.php' script.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability OID: 1.3.6.1.4.1.25623.1.0.108064 Version used: \$Revision: 11863 \$
Product Detection Result Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Method: Tiki Wiki CMS Groupware Version Detection OID: 1.3.6.1.4.1.25623.1.0.901001)
References CVE: CVE-2016-10143 Other: URL: http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-released URL: https://sourceforge.net/p/tikiwiki/code/60308/ URL: https://tiki.org

Medium (CVSS: 6.5) NVT: Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability
Product detection result cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)
Summary In Tiki the user task component is vulnerable to a SQL Injection via the tiki-user_tasks.php show_history parameter.
Vulnerability Detection Result Installed version: 1.9.5 Fixed version: 17.2
Solution Solution type: VendorFix Upgrade to version 17.2 or later.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
Tiki Wiki CMS Groupware prior to version 17.2.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability OID:1.3.6.1.4.1.25623.1.0.141885 Version used: \$Revision: 13115 \$
Product Detection Result Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Method: Tiki Wiki CMS Groupware Version Detection OID: 1.3.6.1.4.1.25623.1.0.901001)
References CVE: CVE-2018-20719 Other: URL: https://blog.ripstech.com/2018/scan-verify-patch-security-issues-in-minute ↪s/

Medium (CVSS: 5.0) NVT: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability
Product detection result cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.↪0.901001)
Summary The host is installed with Tiki Wiki CMS Groupware and is prone to input sanitation weakness vulnerability.
Vulnerability Detection Result Installed version: 1.9.5 Fixed version: 2.2
Impact Successful exploitation could allow arbitrary code execution in the context of an affected site.
Solution Solution type: VendorFix Upgrade to version 2.2 or later.
Affected Software/OS Tiki Wiki CMS Groupware version prior to 2.2 on all running platform
... continues on next page ...

...continued from previous page ...
Vulnerability Insight The vulnerability is due to input validation error in tiki-error.php which fails to sanitise before being returned to the user.
Vulnerability Detection Method Details: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability OID:1.3.6.1.4.1.25623.1.0.800315 Version used: \$Revision: 14010 \$
Product Detection Result Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Method: Tiki Wiki CMS Groupware Version Detection OID: 1.3.6.1.4.1.25623.1.0.901001)
References CVE: CVE-2008-5318, CVE-2008-5319 Other: URL:http://secunia.com/advisories/32341 URL:http://info.tikiwiki.org/tiki-read_article.php?articleId=41

Medium (CVSS: 4.3) NVT: TWiki < 6.1.0 XSS Vulnerability
Product detection result cpe:/a:twiki:twiki:01.Feb.2003 Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
Summary bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 6.1.0
Solution Solution type: VendorFix Update to version 6.1.0 or later.
Affected Software/OS TWiki version 6.0.2 and probably prior.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host.
... continues on next page ...

...continued from previous page ...
Details: TWiki < 6.1.0 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.141830 Version used: 2019-03-26T08:16:24+0000
Product Detection Result Product: cpe:/a:twiki:twiki:01.Feb.2003 Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)
References CVE: CVE-2018-20212 Other: URL:https://seclists.org/fulldisclosure/2019/Jan/7 URL:http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Medium (CVSS: 6.0) NVT: TWiki Cross-Site Request Forgery Vulnerability
Product detection result cpe:/a:twiki:twiki:01.Feb.2003 Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
Summary The host is running TWiki and is prone to Cross-Site Request Forgery Vulnerability.
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 4.3.1
Impact Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Solution Solution type: VendorFix Upgrade to version 4.3.1 or later.
Affected Software/OS TWiki version prior to 4.3.1
Vulnerability Insight Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Details: TWiki Cross-Site Request Forgery Vulnerability OID:1.3.6.1.4.1.25623.1.0.800400 Version used: \$Revision: 12952 \$
Product Detection Result Product: cpe:/a:twiki:twiki:01.Feb.2003 Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)
References CVE: CVE-2009-1339 Other: URL:http://secunia.com/advisories/34880 URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258 URL:http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di ↪ff-cve-2009-1339.txt

Medium (CVSS: 6.8) NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10
Product detection result cpe:/a:twiki:twiki:01.Feb.2003 Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
Summary The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 4.3.2
Impact Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Solution Solution type: VendorFix Upgrade to TWiki version 4.3.2 or later.
Affected Software/OS TWiki version prior to 4.3.2
... continues on next page ...

...continued from previous page ...
Vulnerability Insight Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.
Vulnerability Detection Method Details: TWiki Cross-Site Request Forgery Vulnerability - Sep10 OID:1.3.6.1.4.1.25623.1.0.801281 Version used: \$Revision: 12952 \$
Product Detection Result Product: cpe:/a:twiki:twiki:01.Feb.2003 Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)
References CVE: CVE-2009-4898 Other: URL:http://www.openwall.com/lists/oss-security/2010/08/03/8 URL:http://www.openwall.com/lists/oss-security/2010/08/02/17 URL:http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix URL:http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

[\[return to 10.0.2.4 \]](#)

Medium 2121/tcp

Medium (CVSS: 4.8) NVT: FTP Unencrypted Cleartext Login
Summary The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
Vulnerability Detection Result The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↩. Response(s): Anonymous sessions: 331 Password required for anonymous Non-anonymous sessions: 331 Password required for openvas-vt
Impact An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
Solution Solution type: Mitigation
... continues on next page ...

...continued from previous page ...
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
<p>Vulnerability Detection Method</p> <p>Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.</p> <p>Details: FTP Unencrypted Cleartext Login</p> <p>OID:1.3.6.1.4.1.25623.1.0.108528</p> <p>Version used: \$Revision: 13611 \$</p>
<p>Medium (CVSS: 4.0)</p> <p>NVT: ProFTPD Denial of Service Vulnerability</p>
<p>Product detection result</p> <p>cpe:/a:proftpd:proftpd:1.3.1</p> <p>Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.↔0.900815)</p>
<p>Summary</p> <p>The host is running ProFTPD and is prone to denial of service vulnerability.</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 1.3.1</p> <p>Fixed version: 1.3.2rc3</p>
<p>Impact</p> <p>Successful exploitation will allow attackers to cause a denial of service.</p>
<p>Solution</p> <p>Solution type: VendorFix</p> <p>Upgrade to ProFTPD version 1.3.2rc3 or later.</p>
<p>Affected Software/OS</p> <p>ProFTPD versions prior to 1.3.2rc3</p>
<p>Vulnerability Insight</p> <p>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.</p>
<p>Vulnerability Detection Method</p> <p>Details: ProFTPD Denial of Service Vulnerability</p> <p>OID:1.3.6.1.4.1.25623.1.0.801640</p> <p>Version used: \$Revision: 13602 \$</p>
... continues on next page ...

...continued from previous page ...
Product Detection Result Product: cpe:/a:proftpd:proftpd:1.3.1 Method: ProFTPD Server Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.900815)
References CVE: CVE-2008-7265 Other: URL: http://bugs.proftpd.org/show_bug.cgi?id=3131 URL: http://www.proftpd.org/

Medium (CVSS: 6.8) NVT: ProFTPD Long Command Handling Security Vulnerability
Product detection result cpe:/a:proftpd:proftpd:1.3.1 Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.900815)
Summary The host is running ProFTPD Server, which is prone to cross-site request forgery vulnerability.
Vulnerability Detection Result Installed version: 1.3.1 Fixed version: 1.3.2rc3
Impact This can be exploited to execute arbitrary FTP commands on another user's session privileges.
Solution Solution type: VendorFix Upgrade to the latest version 1.3.2rc3.
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: 13602 \$
... continues on next page ...

...continued from previous page ...
Product Detection Result Product: cpe:/a:proftpd:proftpd:1.3.1 Method: ProFTPD Server Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.900815)
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:1.3.1 Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.↪0.900815)
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: 1.3.1 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.↪..
...continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.100316 Version used: \$Revision: 13602 \$
Product Detection Result Product: cpe:/a:proftpd:proftpd:1.3.1 Method: ProFTPD Server Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.900815)
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

[\[return to 10.0.2.4 \]](#)

Medium 3306/tcp

Medium (CVSS: 6.0) NVT: MySQL Authenticated Access Restrictions Bypass Vulnerability (Linux)
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary The host is running MySQL and is prone to Access Restrictions Bypass Vulnerability.
Vulnerability Detection Result Installed version: 5.0.51a Fixed version: 5.0.88/5.1.41
Impact Successful exploitation could allow users to bypass intended access restrictions by calling CREATE TABLE with DATA DIRECTORY or INDEX DIRECTORY argument referring to a sub-directory.
Solution Solution type: VendorFix Upgrade to MySQL version 5.0.88 or 5.1.41 or 6.0.9-alpha.
Affected Software/OS ... continues on next page ...

...continued from previous page ...
MySQL 5.0.x before 5.0.88, 5.1.x before 5.1.41, 6.0 before 6.0.9-alpha.
Vulnerability Insight The flaw is due to an error in 'sql/sql_table.cc', when the data home directory contains a symlink to a different filesystem.
Vulnerability Detection Method Details: MySQL Authenticated Access Restrictions Bypass Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.801065 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2008-7247 Other: URL: http://lists.mysql.com/commits/59711 URL: http://bugs.mysql.com/bug.php?id=39277 URL: http://marc.info/?l=oss-security&m=125908040022018&w=2 URL: http://dev.mysql.com/downloads

Medium (CVSS: 6.8)
NVT: MySQL Denial Of Service and Spoofing Vulnerabilities
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary The host is running MySQL and is prone to Denial Of Service and Spoofing Vulnerabilities
Vulnerability Detection Result Installed version: 5.0.51a Fixed version: 5.0.88 or 5.1.41
Impact Successful exploitation could allow users to cause a Denial of Service and man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via a crafted certificate.
Solution Solution type: VendorFix
... continues on next page ...

...continued from previous page ...
Upgrade to MySQL version 5.0.88 or 5.1.41.
Affected Software/OS MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 on all running platform.
Vulnerability Insight The flaws are due to: - mysqld does not properly handle errors during execution of certain SELECT statements with subqueries, and does not preserve certain null_value flags during execution of statements that use the 'GeomFromWKB()' function. - An error in 'vio_verify_callback()' function in 'viosslfactories.c', when OpenSSL is used, accepts a value of zero for the depth of X.509 certificates.
Vulnerability Detection Method Details: MySQL Denial Of Service and Spoofing Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.801064 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2009-4019, CVE-2009-4028 Other: URL:http://bugs.mysql.com/47780 URL:http://bugs.mysql.com/47320 URL:http://marc.info/?l=oss-security&m=125881733826437&w=2 URL:http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html URL:http://dev.mysql.com/downloads
Medium (CVSS: 4.0) NVT: MySQL Empty Bit-String Literal Denial of Service Vulnerability
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary This host is running MySQL, which 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 by remote attackers could cause denying access to legitimate users.
Solution Solution type: VendorFix Update to version 5.0.66 or 5.1.26 or 6.0.6 or later.
Affected Software/OS MySQL versions prior to 5.0.x - 5.0.66, 5.1.x - 5.1.26, and 6.0.x - 6.0.5 on all running platform.
Vulnerability Insight Issue is due to error while processing an empty bit string literal via a specially crafted SQL statement.
Vulnerability Detection Method Details: MySQL Empty Bit-String Literal Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.900221 Version used: \$Revision: 14310 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2008-3963 BID:31081 Other: URL: http://secunia.com/advisories/31769/ URL: http://bugs.mysql.com/bug.php?id=35658 URL: http://dev.mysql.com/doc/refman/5.1/en/news-5-1-26.html
Medium (CVSS: 5.0) NVT: MySQL Multiple Denial of Service Vulnerabilities
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary The host is running MySQL and is prone to multiple denial of service vulnerabilities.
Vulnerability Detection Result ... continues on next page ...

...continued from previous page ...
Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation could allow an attacker to cause a denial of service and to execute arbitrary code.
Solution Solution type: VendorFix Upgrade to MySQL version 5.0.92, or 5.1.51 or 5.5.6
Affected Software/OS MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6
Vulnerability Insight The flaws are due to: <ul style="list-style-type: none"> - An error in propagating the type errors, which allows remote attackers to cause a denial of service via crafted arguments to extreme-value functions such as 'LEAST' or 'GREATEST'. - An unspecified error in vectors related to materializing a derived table that required a temporary table for grouping and user variable assignments. - An error in handling prepared statements that uses GROUP_CONCAT with the WITH ROLLUP modifier. - An error in handling a query that uses the GREATEST or LEAST function with a mixed list of numeric and LONGBLOB arguments.
Vulnerability Detection Method Details: MySQL Multiple Denial of Service Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.801571 Version used: \$Revision: 12018 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2010-3833, CVE-2010-3834, CVE-2010-3836, CVE-2010-3837, CVE-2010-3838 BID:43676 Other: <ul style="list-style-type: none"> URL:http://secunia.com/advisories/42875 URL:http://bugs.mysql.com/bug.php?id=54568 URL:http://dev.mysql.com/doc/refman/5.5/en/news-5-5-6.html URL:http://dev.mysql.com/doc/refman/5.0/en/news-5-0-92.html URL:http://dev.mysql.com/doc/refman/5.1/en/news-5-1-51.html URL:http://dev.mysql.com/downloads

<p>Medium (CVSS: 6.5) NVT: MySQL Multiple Vulnerabilities</p>
<p>Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>Summary The host is running MySQL and is prone to multiple vulnerabilities.</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Impact Successful exploitation could allow users to cause a denial of service and to execute arbitrary code.</p>
<p>Solution Solution type: VendorFix Upgrade to MySQL version 5.0.91 or 5.1.47.</p>
<p>Affected Software/OS MySQL 5.0.x before 5.0.91 and 5.1.x before 5.1.47 on all running platform.</p>
<p>Vulnerability Insight The flaws are due to: - An error in 'my_net_skip_rest()' function in 'sql/net_serv.cc' when handling a large number of packets that exceed the maximum length, which allows remote attackers to cause a denial of service (CPU and bandwidth consumption). - buffer overflow when handling 'COM_FIELD_LIST' command with a long table name, allows remote authenticated users to execute arbitrary code. - directory traversal vulnerability when handling a '..' (dot dot) in a table name, which allows remote authenticated users to bypass intended table grants to read field definitions of arbitrary tables.</p>
<p>Vulnerability Detection Method Details: MySQL Multiple Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.801355 Version used: \$Revision: 13960 \$</p>
<p>Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>References ... continues on next page ...</p>

...continued from previous page ...
<p>CVE: CVE-2010-1848, CVE-2010-1849, CVE-2010-1850</p> <p>Other:</p> <p>URL:http://securitytracker.com/alerts/2010/May/1024031.html</p> <p>URL:http://securitytracker.com/alerts/2010/May/1024033.html</p> <p>URL:http://securitytracker.com/alerts/2010/May/1024032.html</p> <p>URL:http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html</p> <p>URL:http://dev.mysql.com/doc/refman/5.0/en/news-5-0-91.html</p> <p>URL:http://dev.mysql.com/downloads</p>

<p>Medium (CVSS: 6.8)</p> <p>NVT: MySQL multiple Vulnerabilities</p>
<p>Product detection result</p> <p>cpe:/a:mysql:mysql:5.0.51a</p> <p>Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>Summary</p> <p>MySQL is prone to a security-bypass vulnerability and to a local privilege-escalation vulnerability.</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 5.0.51a</p> <p>Fixed version: 5.1.41</p>
<p>Impact</p> <p>An attacker can exploit the security-bypass issue to bypass certain security restrictions and obtain sensitive information that may lead to further attacks.</p> <p>Local attackers can exploit the local privilege-escalation issue to gain elevated privileges on the affected computer.</p>
<p>Solution</p> <p>Solution type: VendorFix</p> <p>Updates are available. Please see the references for details.</p>
<p>Affected Software/OS</p> <p>Versions prior to MySQL 5.1.41 are vulnerable.</p>
<p>Vulnerability Detection Method</p> <p>Details: MySQL multiple Vulnerabilities</p> <p>OID:1.3.6.1.4.1.25623.1.0.100356</p> <p>Version used: \$Revision: 11884 \$</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:mysql:mysql:5.0.51a</p> <p>Method: MySQL/MariaDB Detection</p>
... continues on next page ...

...continued from previous page ...
OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2009-4028, CVE-2009-4030 BID:37075, 37076 Other: URL: http://www.securityfocus.com/bid/37076 URL: http://www.securityfocus.com/bid/37075 URL: http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html URL: http://www.mysql.com/
Medium (CVSS: 4.6) NVT: MySQL MyISAM Table Privileges Security Bypass Vulnerability
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary According to its version number, the remote version of MySQL is prone to a security-bypass vulnerability.
Vulnerability Detection Result Installed version: 5.0.51a Fixed version: 4.1.24/5.0.60
Impact An attacker can exploit this issue to gain access to table files created by other users, bypassing certain security restrictions.
Solution Solution type: VendorFix Updates are available, please see the references for more information.
Affected Software/OS This issue affects versions prior to MySQL 4 (prior to 4.1.24) and MySQL 5 (prior to 5.0.60).
Vulnerability Insight NOTE 1: This issue was also assigned CVE-2008-4097 because CVE-2008-2079 was incompletely fixed, allowing symlink attacks. NOTE 2: CVE-2008-4098 was assigned because fixes for the vector described in CVE-2008-4097 can also be bypassed.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
Details: MySQL MyISAM Table Privileges Secuity Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.100156 Version used: \$Revision: 11830 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2008-2079, CVE-2008-4097, CVE-2008-4098 BID:29106 Other: URL: http://www.securityfocus.com/bid/29106

Medium (CVSS: 4.0) NVT: MySQL Mysqld Multiple Denial Of Service Vulnerabilities
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary The host is running MySQL and is prone to multiple denial of service vulnerabilities.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation could allow users to cause a Denial of Service condution.
Solution Solution type: VendorFix Upgrade to MySQL version 5.1.49 or 5.0.92
Affected Software/OS MySQL version 5.1 before 5.1.49 and 5.0 before 5.0.92 on all running platform.
Vulnerability Insight The flaws are due to: - An error in handling of a join query that uses a table with a unique SET column. - An error in handling of 'EXPLAIN' with crafted 'SELECT ... UNION ... ORDER BY (SELECT ... WHERE ...)' statements.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Details: MySQL Mysqld Multiple Denial Of Service Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.801567 Version used: \$Revision: 11997 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2010-3677, CVE-2010-3682 Other: URL:http://bugs.mysql.com/bug.php?id=54477 URL:https://bugzilla.redhat.com/show_bug.cgi?id=628172 URL:http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html URL:http://www.openwall.com/lists/oss-security/2010/09/28/10 URL:http://dev.mysql.com/downloads

Medium (CVSS: 4.6) NVT: MySQL Privilege Escalation Vulnerability - Linux
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary This host is running MySQL and is prone to privilege escalation vulnerability.
Vulnerability Detection Result Installed version: 5.0.51a Fixed version: 5.0.67
Impact Successful exploitation of this vulnerability will allow an authenticated user to use the DATA DIRECTORY and INDEX DIRECTORY options to possibly bypass privilege checks.
Solution Solution type: VendorFix Upgrade to MySQL version 5.0.67.
Affected Software/OS MySQL version before 5.0.67 on Linux
... continues on next page ...

...continued from previous page ...
Vulnerability Insight The flaw exists due to table creation option allows the use of the MySQL data directory in DATA DIRECTORY and INDEX DIRECTORY options.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: MySQL Privilege Escalation Vulnerability - Linux OID:1.3.6.1.4.1.25623.1.0.811630 Version used: \$Revision: 11923 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2008-4098 BID:29106 Other: URL: https://bugs.mysql.com/bug.php?id=32167

Medium (CVSS: 5.0) NVT: MySQL/MariaDB Authentication Error Message User Enumeration Vulnerability
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary The host is running MySQL/MariaDB and is prone to user enumeration vulnerability.
Vulnerability Detection Result Installed version: 5.0.51a Fixed version: See references
Impact Successful exploitation allows attackers to obtain valid usernames, which may aid them in brute-force password cracking or other attacks.
Solution Solution type: VendorFix For MariaDB upgrade to 5.5.29, 5.3.12, 5.2.14 or later. For MySQL apply the updates from vendor.
... continues on next page ...

...continued from previous page ...
Affected Software/OS MySQL version 5.5.19 and possibly other versions MariaDB 5.5.28a, 5.3.11, 5.2.13, 5.1.66 and possibly other versions
Vulnerability Insight MySQL server will respond with a different message than Access Denied, when attacker authenticates using an incorrect password with the old authentication mechanism MySQL 4.x and below to a MySQL 5.x server.
Vulnerability Detection Method Details: MySQL/MariaDB Authentication Error Message User Enumeration Vulnerability OID:1.3.6.1.4.1.25623.1.0.802046 Version used: \$Revision: 12175 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2012-5615 BID:56766 Other: URL:http://secunia.com/advisories/51427 URL:http://www.exploit-db.com/exploits/23081 URL:https://mariadb.atlassian.net/browse/MDEV-3909 URL:https://bugzilla.redhat.com/show_bug.cgi?id=882608 URL:http://www.openwall.com/lists/oss-security/2012/12/02/3 URL:http://www.openwall.com/lists/oss-security/2012/12/02/4 URL:https://mariadb.org/ URL:https://www.mysql.com/
Medium (CVSS: 4.0) NVT: Oracle MySQL 'TEMPORARY InnoDB' Tables Denial Of Service Vulnerability
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary MySQL is prone to a denial-of-service vulnerability.
Vulnerability Detection Result Installed version: 5.0.51a
... continues on next page ...

...continued from previous page ...	
Fixed version:	5.1.49
Impact An attacker can exploit these issues to crash the database, denying access to legitimate users.	
Solution Solution type: VendorFix Updates are available. Please see the references for more information.	
Affected Software/OS This issues affect versions prior to MySQL 5.1.49.	
Vulnerability Detection Method Details: Oracle MySQL 'TEMPORARY InnoDB' Tables Denial Of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.100763 Version used: \$Revision: 11830 \$	
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)	
References CVE: CVE-2010-3680 BID:42598 Other: URL: https://www.securityfocus.com/bid/42598 URL: http://bugs.mysql.com/bug.php?id=54044 URL: http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html URL: http://www.mysql.com/	

Medium (CVSS: 5.0) NVT: Oracle MySQL Denial Of Service Vulnerability Feb17 (Linux)	
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)	
Summary This host is running Oracle MySQL and is prone to denial-of-service vulnerability.	
Vulnerability Detection Result Installed version: 5.0.51a Fixed version: 5.6.21	
... continues on next page ...	

...continued from previous page ...	
Installation	
path / port:	3306/tcp
Impact	Successful exploitation of this vulnerability will allow attackers to cause crash of applications using that MySQL client.
Solution	
Solution type:	VendorFix
	Upgrade to Oracle MySQL version 5.6.21 or 5.7.5 or later.
Affected Software/OS	
	Oracle MySQL version before 5.6.21 and 5.7.x before 5.7.5 on Linux
Vulnerability Insight	
	Multiple errors exists as, - In sql-common/client.c script 'mysql_prune_stmt_list' function, the for loop adds elements to pruned_list without removing it from the existing list. - If application gets disconnected just before it tries to prepare a new statement, 'mysql_prune_stmt_list' tries to detach all previously prepared statements.
Vulnerability Detection Method	
	Checks if a vulnerable version is present on the target host. Details: Oracle MySQL Denial Of Service Vulnerability Feb17 (Linux) OID:1.3.6.1.4.1.25623.1.0.810604 Version used: \$Revision: 12983 \$
Product Detection Result	
	Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References	
	CVE: CVE-2017-3302 Other: URL: https://bugs.mysql.com/bug.php?id=63363 URL: https://bugs.mysql.com/bug.php?id=70429 URL: http://www.openwall.com/lists/oss-security/2017/02/11/11
Medium (CVSS: 4.0) NVT: Oracle MySQL Prior to 5.1.49 Multiple Denial Of Service Vulnerabilities	
Product detection result	
	cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
... continues on next page ...	

...continued from previous page ...
<p>Summary MySQL is prone to a denial-of-service vulnerability. An attacker can exploit this issue to crash the database, denying access to legitimate users. This issue affects versions prior to MySQL 5.1.49.</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Solution Solution type: VendorFix Updates are available. Please see the references for more information.</p>
<p>Vulnerability Detection Method Details: Oracle MySQL Prior to 5.1.49 Multiple Denial Of Service Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100785 Version used: \$Revision: 13960 \$</p>
<p>Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
<p>References CVE: CVE-2010-3677 BID:42646, 42633, 42643, 42598, 42596, 42638, 42599, 42625 Other: URL:https://www.securityfocus.com/bid/42646 URL:https://www.securityfocus.com/bid/42633 URL:https://www.securityfocus.com/bid/42643 URL:https://www.securityfocus.com/bid/42598 URL:https://www.securityfocus.com/bid/42596 URL:https://www.securityfocus.com/bid/42638 URL:https://www.securityfocus.com/bid/42599 URL:https://www.securityfocus.com/bid/42625 URL:http://bugs.mysql.com/bug.php?id=54575 URL:http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html URL:http://www.mysql.com/</p>
<p>Medium (CVSS: 5.0) NVT: Oracle MySQL Prior to 5.1.51 Multiple Denial Of Service Vulnerabilities</p>
<p>Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)</p>
... continues on next page ...

...continued from previous page ...
Summary MySQL is prone to multiple denial-of-service vulnerabilities.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact An attacker can exploit these issues to crash the database, denying access to legitimate users.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS These issues affect versions prior to MySQL 5.1.51.
Vulnerability Detection Method Details: Oracle MySQL Prior to 5.1.51 Multiple Denial Of Service Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100900 Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2010-3833, CVE-2010-3834, CVE-2010-3835, CVE-2010-3836, CVE-2010-3837, ↗CVE-2010-3838, CVE-2010-3839, CVE-2010-3840 BID:43676 Other: URL: https://www.securityfocus.com/bid/43676 URL: http://dev.mysql.com/doc/refman/5.1/en/news-5-1-51.html URL: http://www.mysql.com/
Medium (CVSS: 4.0) NVT: Oracle Mysql Security Updates (jan2012-366304) 03 - Linux
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
... continues on next page ...

...continued from previous page ...
Summary This host is running Oracle MySQL and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.0.51a Fixed version: Apply the patch Installation path / port: 3306/tcp
Impact Successful exploitation of these vulnerabilities will allow remote attackers to affect integrity, availability and confidentiality.
Solution Solution type: VendorFix Apply the patch from the referenced advisory.
Affected Software/OS Oracle MySQL version 5.0.x, 5.1.x and 5.5.x on Linux
Vulnerability Insight Multiple flaws exists due to multiple unspecified errors in MySQL Server.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle Mysql Security Updates (jan2012-366304) 03 - Linux OID:1.3.6.1.4.1.25623.1.0.812347 Version used: \$Revision: 12983 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2012-0075, CVE-2012-0484, CVE-2012-0114, CVE-2012-0490 BID:51526, 51515, 51520, 51524 Other: URL: http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
Medium (CVSS: 4.0) NVT: Oracle Mysql Security Updates (jan2012-366304) 04 - Linux
Product detection result cpe:/a:mysql:mysql:5.0.51a
... continues on next page ...

...continued from previous page ...
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary This host is running Oracle MySQL and is prone to multiple vulnerabilities.
Vulnerability Detection Result Installed version: 5.0.51a Fixed version: Apply the patch Installation path / port: 3306/tcp
Impact Successful exploitation of this vulnerability will allow remote users to affect integrity, availability and confidentiality.
Solution Solution type: VendorFix Apply the patch from the referenced advisory.
Affected Software/OS Oracle MySQL version 5.0.x and 5.1.x on Linux
Vulnerability Insight Multiple flaws exists due to multiple unspecified errors in MySQL Server.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Oracle Mysql Security Updates (jan2012-366304) 04 - Linux OID:1.3.6.1.4.1.25623.1.0.812349 Version used: \$Revision: 12983 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2012-0087, CVE-2012-0102, CVE-2012-0101 BID:51509, 51502, 51505 Other: URL: http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

[\[return to 10.0.2.4 \]](#)

Medium 5432/tcp

Medium (CVSS: 6.5) NVT: PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary PostgreSQL is prone to a buffer-overflow vulnerability because the application fails to perform adequate boundary checks on user-supplied data.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: See references
Impact Attackers can exploit this issue to execute arbitrary code with elevated privileges or crash the affected application.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS PostgreSQL version 8.0.x, 8.1.x, 8.3.x is vulnerable. Other versions may also be affected.
Vulnerability Detection Method Details: PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.100470 Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2010-0442 BID:37973 Other: URL:http://www.postgresql.org/ URL:http://www.securityfocus.com/bid/37973 URL:http://xforce.iss.net/xforce/xfdb/55902 URL:http://intevydis.blogspot.com/2010/01/postgresql-8023-bitsubstr-overflow. ↪html

Medium (CVSS: 6.5) NVT: PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary PostgreSQL is prone to a buffer-overflow vulnerability because the application fails to perform adequate boundary checks on user-supplied data. The issue affects the 'intarray' module.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: See references
Impact An authenticated attacker can leverage this issue to execute arbitrary code within the context of the vulnerable 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 The issue affect versions prior to 8.2.20, 8.3.14, 8.4.7, and 9.0.3.
Vulnerability Detection Method Details: PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.103054 Version used: \$Revision: 11997 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2010-4015 BID:46084 Other: URL: https://www.securityfocus.com/bid/46084 URL: http://www.postgresql.org/ URL: http://www.postgresql.org/about/news.1289

Medium (CVSS: 5.5) NVT: PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary PostgreSQL is prone to an unauthorized-access vulnerability.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: See references
Impact Attackers can exploit this issue to reset special parameter settings only a root user should be able to modify. This may aid in further attacks.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS This issue affects versions prior to the following PostgreSQL versions: 7.4.29 8.0.25 8.1.21 8.2.17 8.3.11 8.4.4
Vulnerability Detection Method Details: PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability OID:1.3.6.1.4.1.25623.1.0.100648 Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2010-1975 BID:40304 Other: URL: http://www.securityfocus.com/bid/40304
... continues on next page ...

...continued from previous page ...
URL: http://www.postgresql.org/docs/current/static/release-8-4-4.html
URL: http://www.postgresql.org/docs/current/static/release-8-2-17.html
URL: http://www.postgresql.org/docs/current/static/release-8-1-21.html
URL: http://www.postgresql.org/docs/current/static/release-8-3-11.html
URL: http://www.postgresql.org/
URL: http://www.postgresql.org/docs/current/static/release-8-0-25.html
URL: http://www.postgresql.org/docs/current/static/release-7-4-29.html

Medium (CVSS: 6.5) NVT: PostgreSQL Code Injection and Denial of Service Vulnerabilities (Linux)
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary This host is running PostgreSQL and is prone to code injection and denial of service vulnerabilities.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: 9.1.23
Impact Successful exploitation will allow a remote attacker to inject code and cause the server to crash.
Solution Solution type: VendorFix Upgrade to version 9.1.23 or 9.2.18 or 9.3.14 or 9.4.9 or 9.5.4 or higher.
Affected Software/OS PostgreSQL version before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 on linux.
Vulnerability Insight Multiple flaws are due to - An error in certain nested CASE expressions. - Improper sanitization of input passed to database and role names.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PostgreSQL Code Injection and Denial of Service Vulnerabilities (Linux) OID:1.3.6.1.4.1.25623.1.0.808665 Version used: \$Revision: 11961 \$
... continues on next page ...

...continued from previous page ...
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2016-5423, CVE-2016-5424 BID: 92433, 92435 Other: URL: https://www.postgresql.org/about/news/1688/ URL: http://www.postgresql.org/download

Medium (CVSS: 4.0) NVT: PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary PostgreSQL is prone to a remote denial-of-service vulnerability.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: See references
Impact Exploiting this issue may allow attackers to terminate connections to the PostgreSQL server, denying service to legitimate users.
Solution Solution type: VendorFix Updates are available. Update to newer Version.
Vulnerability Detection Method Details: PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability OID: 1.3.6.1.4.1.25623.1.0.100157 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
... continues on next page ...

...continued from previous page ...
References CVE: CVE-2009-0922 BID:34090 Other: URL: http://www.securityfocus.com/bid/34090 URL: http://www.postgresql.org/
Medium (CVSS: 5.0) NVT: PostgreSQL Multiple Information Disclosure Vulnerabilities - May17 (Linux)
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary This host is running PostgreSQL and is prone to multiple information disclosure vulnerabilities.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: 9.2.21
Impact Successful exploitation will allow an unprivileged attacker to steal some information.
Solution Solution type: VendorFix Upgrade to PostgreSQL version 9.2.21 or 9.3.17 or 9.4.12 or 9.5.7 or 9.6.3 or later.
Affected Software/OS PostgreSQL version before 9.2.21, 9.3.x before 9.3.17, 9.4.x before 9.4.12, 9.5.x before 9.5.7, and 9.6.x before 9.6.3 on Linux.
Vulnerability Insight Multiple flaws are due to, - Some selectivity estimation functions did not check user privileges before providing information from pg_statistic, possibly leaking information. - An error in 'pg_user_mappings' view.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PostgreSQL Multiple Information Disclosure Vulnerabilities - May17 (Linux) OID:1.3.6.1.4.1.25623.1.0.810990 Version used: \$Revision: 11935 \$
Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2017-7484, CVE-2017-7486 Other: URL: https://www.postgresql.org/about/news/1746 URL: http://www.postgresql.org/download

Medium (CVSS: 6.8) NVT: PostgreSQL Multiple Security Vulnerabilities
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary PostgreSQL is prone to multiple security vulnerabilities, including a denial-of-service issue, a privilege-escalation issue, and an authentication-bypass issue.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: See references
Impact Attackers can exploit these issues to shut down affected servers, perform certain actions with elevated privileges, and bypass authentication mechanisms to perform unauthorized actions. Other attacks may also be possible.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Vulnerability Detection Method Details: PostgreSQL Multiple Security Vulnerabilities OID: 1.3.6.1.4.1.25623.1.0.100273 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
... continues on next page ...

...continued from previous page ...

References

CVE: CVE-2009-3229, CVE-2009-3230, CVE-2009-3231

BID:36314

Other:

URL:<http://www.securityfocus.com/bid/36314>URL:https://bugzilla.redhat.com/show_bug.cgi?id=522085#c1URL:<http://www.postgresql.org/>URL:<http://www.postgresql.org/support/security>URL:<http://permalink.gmane.org/gmane.comp.security.oss.general/2088>

Medium (CVSS: 6.5)

NVT: PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability

Product detection result

cpe:/a:postgresql:postgresql:8.3.1

Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary

PostgreSQL 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.

PostgreSQL is also prone to a local privilege-escalation vulnerability.

Vulnerability Detection Result

Installed version: 8.3.1

Fixed version: See references

Impact

Successfully exploiting this issue allows attackers to perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks.

Exploiting the privilege-escalation vulnerability allows local attackers to gain elevated privileges.

Solution**Solution type:** VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

PostgreSQL versions prior to 8.4.2, 8.3.9, 8.2.15, 8.1.19, 8.0.23, and 7.4.27 are vulnerable to this issue.

Vulnerability Detection Method

Details: PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnera.

↔..

OID:1.3.6.1.4.1.25623.1.0.100400

Version used: \$Revision: 14031 \$

...continues on next page ...

...continued from previous page ...
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2009-4034, CVE-2009-4136 BID:37334, 37333 Other: URL:http://www.securityfocus.com/bid/37334 URL:http://www.securityfocus.com/bid/37333 URL:http://www.postgresql.org URL:http://www.postgresql.org/support/security URL:http://www.postgresql.org/about/news.1170

Medium (CVSS: 6.0) NVT: PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary PostgreSQL is prone to a local privilege-escalation vulnerability.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: See references
Impact Exploiting this issue allows local attackers to gain elevated privileges and execute arbitrary commands with the privileges of the victim.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS Versions prior to PostgreSQL 9.0.1 are vulnerable.
Vulnerability Detection Method Details: PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability OID:1.3.6.1.4.1.25623.1.0.100843
... continues on next page ...

...continued from previous page ...
Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2010-3433 BID: 43747 Other: URL: https://www.securityfocus.com/bid/43747 URL: http://www.postgresql.org/docs/9.0/static/release-9-0-1.html URL: http://www.postgresql.org URL: http://www.postgresql.org/support/security

Medium (CVSS: 4.3)
NVT: PostgreSQL Remote Denial Of Service Vulnerability June15 (Linux)
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary This host is running PostgreSQL and is prone to remote denial of service vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow a remote attacker to crash the program.
Solution Solution type: VendorFix Upgrade to version 9.0.20, 9.1.16, 9.2.11, 9.3.7, 9.4.2 or later.
Affected Software/OS PostgreSQL version before 9.0.20, 9.1.x before 9.1.16, 9.2.x before 9.2.11, 9.3.x before 9.3.7, and 9.4.x before 9.4.2 on Linux.
Vulnerability Insight Flaw is triggered when a timeout interrupt is fired partway through the session shutdown sequence.
... continues on next page ...

...continued from previous page...
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PostgreSQL Remote Denial Of Service Vulnerability June15 (Linux) OID:1.3.6.1.4.1.25623.1.0.805805 Version used: \$Revision: 11872 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2015-3165 BID:74787 Other: URL: http://www.postgresql.org/about/news/1587 URL: http://www.postgresql.org/download

Medium (CVSS: 5.0) NVT: SSL/TLS: Certificate Expired
Summary The remote server's SSL/TLS certificate has already expired.
Vulnerability Detection Result The certificate of the remote service expired on 2010-04-16 14:07:45. Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6 ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX subject alternative names (SAN): None issued by ..: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6 ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX serial: 00FAF93A4C7FB6B9CC valid from : 2010-03-17 14:07:45 UTC valid until: 2010-04-16 14:07:45 UTC fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436 ↪DE813CC
Solution Solution type: Mitigation
... continues on next page ...

...continued from previous page ...
Replace the SSL/TLS certificate by a new one.
Vulnerability Insight This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.
Vulnerability Detection Method Details: SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: \$Revision: 11103 \$
Medium (CVSS: 4.0) NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
Summary The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.
Vulnerability Detection Result The following certificates are part of the certificate chain but using insecure ↪signature algorithms: Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173 ↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic ↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi ↪ng outside US,C=XX Signature Algorithm: sha1WithRSAEncryption
Solution Solution type: Mitigation Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.
Vulnerability Insight The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1
... continues on next page ...

...continued from previous page ...	
or fingerprint1,Fingerprint2	
Vulnerability Detection Method Check which hashing algorithm was used to sign the remote SSL/TLS certificate. Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm OID:1.3.6.1.4.1.25623.1.0.105880 Version used: \$Revision: 11524 \$	
References Other: URL: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/	
Medium (CVSS: 4.3) NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	
Summary It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	
Vulnerability Detection Result In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto ↪col and supports one or more ciphers. Those supported ciphers can be found in ↪the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.8 ↪02067) NVT.	
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.	
Solution Solution type: Mitigation It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.	
Affected Software/OS All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.	
Vulnerability Insight The SSLv2 and SSLv3 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)	
Vulnerability Detection Method ... continues on next page ...	

...continued from previous page ...	
Check the used protocols of the services provided by this system. Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012 Version used: \$Revision: 5547 \$	
References CVE: CVE-2016-0800, CVE-2014-3566 Other: URL: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report URL: https://bettercrypto.org/ URL: https://mozilla.github.io/server-side-tls/ssl-config-generator/ URL: https://drownattack.com/ URL: https://www.imperialviolet.org/2014/10/14/poodle.html	
Medium (CVSS: 4.0) NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	
Summary The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).	
Vulnerability Detection Result Server Temporary Key Size: 1024 bits	
Impact An attacker might be able to decrypt the SSL/TLS communication offline.	
Solution Solution type: Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.	
Vulnerability Insight The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.	
Vulnerability Detection Method Checks the DHE temporary public key size. Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↪... OID:1.3.6.1.4.1.25623.1.0.106223 Version used: \$Revision: 12865 \$	
... continues on next page ...	

...continued from previous page ...

References**Other:**URL:<https://weakdh.org/>URL:<https://weakdh.org/sysadmin.html>

Medium (CVSS: 6.8)

NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Summary

OpenSSL is prone to security-bypass vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution**Solution type:** VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

Vulnerability Insight

OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method

Send two SSL ChangeCipherSpec request and check the response.

Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

OID:1.3.6.1.4.1.25623.1.0.105042

Version used: \$Revision: 12865 \$

References

CVE: CVE-2014-0224

BID:67899

Other:URL:<https://www.openssl.org/news/secadv/20140605.txt>URL:<http://www.securityfocus.com/bid/67899>URL:<http://openssl.org/>

Medium (CVSS: 4.3) NVT: SSL/TLS: Report Weak Cipher Suites
Summary This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
Vulnerability Detection Result 'Weak' cipher suites accepted by this service via the SSLv3 protocol: TLS_RSA_WITH_RC4_128_SHA 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_SHA
Solution Solution type: Mitigation The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.
Vulnerability Insight These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000). - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong
Vulnerability Detection Method Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: \$Revision: 11135 \$
References CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000 Other: URL: https://www.bsi.bund.de/SharedDocs/Warntmeldungen/DE/CB/warntmeldung_cb-k16-1465_update_6.html URL: https://bettercrypto.org/ URL: https://mozilla.github.io/server-side-tls/ssl-config-generator/

Medium (CVSS: 4.3) NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
... continues on next page ...

...continued from previous page...	
Summary	This host is prone to an information disclosure vulnerability.
Vulnerability Detection Result	Vulnerability was detected according to the Vulnerability Detection Method.
Impact	Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
Solution	Solution type: Mitigation Possible Mitigations are: <ul style="list-style-type: none"> - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
Vulnerability Insight	The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
Vulnerability Detection Method	Evaluate previous collected information about this service. Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↔.. OID:1.3.6.1.4.1.25623.1.0.802087 Version used: \$Revision: 11402 \$
References	CVE: CVE-2014-3566 BID:70574 Other: <ul style="list-style-type: none"> URL:https://www.openssl.org/~bodo/ssl-poodle.pdf URL:https://www.imperialviolet.org/2014/10/14/poodle.html URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit-↔ing-ssl-30.html

[\[return to 10.0.2.4 \]](#)

Medium 6667/tcp

Medium (CVSS: 6.8)
NVT: UnrealIRCd Authentication Spoofing Vulnerability
Product detection result
... continues on next page ...

...continued from previous page...
cpe:/a:unrealircd:unrealircd:3.2.8.1 Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)
Summary This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability.
Vulnerability Detection Result Installed version: 3.2.8.1 Fixed version: 3.2.10.7
Impact Successful exploitation of this vulnerability will allow remote attackers to spoof certificate fingerprints and consequently log in as another user.
Solution Solution type: VendorFix Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.
Affected Software/OS UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.
Vulnerability Insight The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: UnrealIRCd Authentication Spoofing Vulnerability OID:1.3.6.1.4.1.25623.1.0.809883 Version used: \$Revision: 11874 \$
Product Detection Result Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection OID: 1.3.6.1.4.1.25623.1.0.809884)
References CVE: CVE-2016-7144 BID:92763 Other: URL: http://seclists.org/oss-sec/2016/q3/420 URL: http://www.openwall.com/lists/oss-security/2016/09/05/8 URL: https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86bc50ba1a34a766 URL: https://bugs.unrealircd.org/main_page.php

[\[return to 10.0.2.4 \]](#)

Medium 445/tcp

Medium (CVSS: 6.8) NVT: Samba 'fd_open_atomic infinite loop' Denial-of-Service Vulnerability
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary This host is running Samba and is prone to denial-of-service vulnerability.
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 4.4.10 Installation path / port: 445/tcp
Impact Successfully exploiting this issue will allow remote attackers to conduct a denial-of-service condition(infinite loop with high CPU usage and memory consumption).
Solution Solution type: VendorFix Upgrade to Samba 4.4.10 or 4.5.6 or later.
Affected Software/OS Samba versions before 4.4.10 and 4.5.x before 4.5.6
Vulnerability Insight The flaw exists due to error in smbd which enters infinite loop when trying to open an invalid symlink with O_CREAT.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba 'fd_open_atomic infinite loop' Denial-of-Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.811083 Version used: \$Revision: 14300 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2017-9461
... continues on next page ...

...continued from previous page ...

Other:URL: https://bugzilla.samba.org/show_bug.cgi?id=12572URL: <https://git.samba.org/?p=samba.git;a=commit;h=10c3e3923022485c720f322ca4f0aca5d7501310>URL: <https://www.samba.org>

Medium (CVSS: 5.0)

NVT: Samba 'FD_SET' Memory Corruption Vulnerability

Product detection result

cpe:/a:samba:samba:3.0.20

Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary

Samba is prone to a memory-corruption vulnerability.

Vulnerability Detection Result

Installed version: 3.0.20

Fixed version: 3.5.7

Installation

path / port: 445/tcp

Impact

An attacker can exploit this issue to crash the application or cause the application to enter an infinite loop. Due to the nature of this issue, arbitrary code execution may be possible but this has not been confirmed.

Solution**Solution type:** VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Samba versions prior to 3.5.7 are vulnerable.

Vulnerability Detection Method

Details: Samba 'FD_SET' Memory Corruption Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.103095

Version used: \$Revision: 10398 \$

Product Detection Result

Product: cpe:/a:samba:samba:3.0.20

Method: SMB NativeLanMan

OID: 1.3.6.1.4.1.25623.1.0.102011)

... continues on next page ...

...continued from previous page ...

References

CVE: CVE-2011-0719

BID: 46597

Other:

URL: <https://www.securityfocus.com/bid/46597>URL: <http://www.samba.org>URL: <http://samba.org/samba/security/CVE-2011-0719.html>

Medium (CVSS: 6.8)

NVT: Samba 'mount.cifs' Utility Local Privilege Escalation Vulnerability

Product detection result

cpe:/a:samba:samba:3.0.20

Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary

Samba is prone to a local privilege-escalation vulnerability in the 'mount.cifs' utility.

Vulnerability Detection Result

Installed version: 3.0.20

Fixed version: 3.4.6

Installation

path / port: 445/tcp

Impact

Local attackers can exploit this issue to gain elevated privileges on affected computers.

Solution**Solution type:** VendorFix

Updates are available. Please see the references for more information.

Vulnerability Detection Method

Details: Samba 'mount.cifs' Utility Local Privilege Escalation Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.100476

Version used: \$Revision: 10398 \$

Product Detection Result

Product: cpe:/a:samba:samba:3.0.20

Method: SMB NativeLanMan

OID: 1.3.6.1.4.1.25623.1.0.102011)

References

CVE: CVE-2009-3297, CVE-2010-0787

BID: 37992

Other:

... continues on next page ...

...continued from previous page ...

URL:<http://www.securityfocus.com/bid/37992>URL:<http://www.samba.org>

Medium (CVSS: 6.8)

NVT: Samba Badlock Critical Vulnerability

Product detection result

cpe:/a:samba:samba:3.0.20

Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary

This host is running Samba and is prone to badlock vulnerability.

Vulnerability Detection Result

Installed version: 3.0.20

Fixed version: 4.2.11 or 4.3.8 or 4.4.2, or later

Installation

path / port: 445/tcp

Impact

Successful exploitation of this vulnerability leads to Man-in-the-middle (MITM) attacks, to causes denial of service, to spoof and to obtain sensitive session information.

Solution**Solution type:** VendorFix

Upgrade to samba version 4.2.11, or 4.3.8, or 4.4.2, or later.

Affected Software/OS

Samba versions 3.0.x through 4.4.1

- —

NOTE: Samba versions 4.2.11, 4.3.8 are not affected

- —

Vulnerability Insight

The multiple flaws are due to,

- The Multiple errors in DCE-RPC code.
- A spoofing Vulnerability in NETLOGON.
- The LDAP implementation did not enforce integrity protection for LDAP connections.
- The SSL/TLS certificates are not validated in certain connections.
- Not enforcing Server Message Block (SMB) signing for clients using the SMB1 protocol.
- An integrity protection for IPC traffic is not enabled by default
- The MS-SAMR and MS-LSAD protocol implementations mishandle DCERPC connections.
- An error in the implementation of NTLMSSP authentication.

Vulnerability Detection Method

... continues on next page ...

...continued from previous page ...
<p>Checks if a vulnerable version is present on the target host. Details: Samba Badlock Critical Vulnerability OID:1.3.6.1.4.1.25623.1.0.807646 Version used: \$Revision: 11772 \$</p>
<p>Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)</p>
<p>References CVE: CVE-2016-2118, CVE-2015-5370, CVE-2016-2110, CVE-2016-2111, CVE-2016-2112, ↔CVE-2016-2113, CVE-2016-2114, CVE-2016-2115, CVE-2016-0128 Other: URL:http://badlock.org/ URL:http://thehackernews.com/2016/03/windows-samba-vulnerability.html</p>

<p>Medium (CVSS: 5.8) NVT: Samba Format String Vulnerability</p>
<p>Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)</p>
<p>Summary The host has Samba installed and is prone to Security Bypass Vulnerability.</p>
<p>Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 3.0.35/3.2.13/3.3.6 Installation path / port: 445/tcp</p>
<p>Impact When dos filemode is set to yes in the smb.conf, attackers can exploit this issue to bypass certain security restrictions and compromise a user's system.</p>
<p>Solution Solution type: VendorFix Upgrade to version 3.3.6 or later.</p>
<p>Affected Software/OS Samba 3.0.0 before 3.0.35 on Linux. Samba 3.1.x on Linux. Samba 3.2.4 before 3.2.13 on Linux.</p>
... continues on next page ...

...continued from previous page ...
Samba 3.3.0 before 3.3.6 on Linux.
Vulnerability Insight The flaw is due to uninitialised memory access error in 'smbd' when denying attempts to modify a restricted access control list. This can be exploited to modify the ACL of an already writable file without required permissions.
Vulnerability Detection Method Details: Samba Format String Vulnerability OID: 1.3.6.1.4.1.25623.1.0.900685 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2009-1888 BID: 35472 Other: URL: http://secunia.com/advisories/35539 URL: http://www.vupen.com/english/advisories/2009/1664

Medium (CVSS: 6.0) NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability (Version Check)
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: See referenced vendor advisory Installation path / port: 445/tcp
Impact An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.
... continues on next page ...

...continued from previous page ...
Solution Solution type: VendorFix Updates are available. Please see the referenced vendor advisory.
Affected Software/OS This issue affects Samba 3.0.0 to 3.0.25rc3.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba MS-RPC Remote Shell Command Execution Vulnerability (Version Check) OID:1.3.6.1.4.1.25623.1.0.108012 Version used: \$Revision: 12363 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2007-2447 BID:23972 Other: URL: http://www.securityfocus.com/bid/23972 URL: https://www.samba.org/samba/security/CVE-2007-2447.html

Medium (CVSS: 6.0) NVT: Samba multiple vulnerabilities
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary Samba is prone to multiple vulnerabilities including a vulnerability that may allow attackers to bypass certain security restrictions, an information-disclosure vulnerability and a remote denial-of-service vulnerability.
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 3.0.37/3.2.15/3.3.8/3.4.2 Installation path / port: 445/tcp
Impact ... continues on next page ...

...continued from previous page ...
Successful exploits may allow attackers to gain access to resources that aren't supposed to be shared, allow attackers to obtain sensitive information that may aid in further attacks and to cause the application to consume excessive CPU resources, denying service to legitimate users.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS Versions prior to Samba 3.4.2, 3.3.8, 3.2.15, and 3.0.37 are vulnerable.
Vulnerability Detection Method Details: Samba multiple vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100306 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2009-2813, CVE-2009-2948, CVE-2009-2906 BID:36363, 36572, 36573 Other: URL:http://www.securityfocus.com/bid/36363 URL:http://www.securityfocus.com/bid/36573 URL:http://www.securityfocus.com/bid/36572 URL:http://www.samba.org/samba/security/CVE-2009-2813.html URL:http://www.samba.org/samba/security/CVE-2009-2948.html URL:http://www.samba.org/samba/security/CVE-2009-2906.html URL:http://www.samba.org/samba/history/security.html URL:http://us1.samba.org/samba/
Medium (CVSS: 4.8) NVT: Samba Server 'SMB1' Memory Information Leak Vulnerability
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary This host is running Samba and is prone to memory information leak vulnerability.
Vulnerability Detection Result
... continues on next page ...

...continued from previous page ...	
Installed version: 3.0.20 Fixed version: 4.4.16 Installation path / port: 445/tcp	
Impact Successful exploitation will allow a client with write access to a share can cause server memory contents to be written into a file or printer.	
Solution Solution type: VendorFix Upgrade to Samba 4.6.8, 4.5.14 and 4.4.16 or later.	
Affected Software/OS Samba versions before 4.4.16, 4.5.0 before 4.5.14, and 4.6.0 before 4.6.8.	
Vulnerability Insight A server memory information leak bug over SMB1 if a client can write data to a share. Some SMB1 write requests were not correctly range checked to ensure the client had sent enough data to fulfill the write.	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Samba Server 'SMB1' Memory Information Leak Vulnerability OID:1.3.6.1.4.1.25623.1.0.811905 Version used: \$Revision: 11983 \$	
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)	
References CVE: CVE-2017-12163 BID:100925 Other: URL: https://www.samba.org/samba/security/CVE-2017-12163.html	
Medium (CVSS: 5.0) NVT: Samba winbind Daemon Denial of Service Vulnerability	
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)	
... continues on next page ...	

...continued from previous page ...
Summary This host is installed with Samba for Linux and is prone to Winbind daemon Denial of Service Vulnerability.
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 3.0.32 Installation path / port: 445/tcp
Impact Successful exploitation will let the attacker crash the application.
Solution Solution type: VendorFix Upgrade to version 3.0.32 or later.
Affected Software/OS Samba version prior to 3.0.32.
Vulnerability Insight This flaw is due to a race condition in the winbind daemon which allows remote attackers to cause denial of service through unspecified vectors related to an unresponsive child process.
Vulnerability Detection Method Details: Samba winbind Daemon Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.800711 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References Other: URL: http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0308 URL: http://www.samba.org/samba/history/samba-3.0.32.html URL: http://www.securityfocus.com/archive/1/archive/1/497941/100/0/threaded

[\[return to 10.0.2.4 \]](#)

Medium 5900/tcp

Medium (CVSS: 4.8) NVT: VNC Server Unencrypted Data Transmission
Summary The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.
Vulnerability Detection Result The VNC server provides the following insecure or cryptographically weak Security Type(s): 2 (VNC authentication)
Impact An attacker can uncover sensitive data by sniffing traffic to the VNC server.
Solution Solution type: Mitigation Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.
Vulnerability Detection Method Details: VNC Server Unencrypted Data Transmission OID:1.3.6.1.4.1.25623.1.0.108529 Version used: \$Revision: 13014 \$
References Other: URL: https://tools.ietf.org/html/rfc6143#page-10

[\[return to 10.0.2.4 \]](#)

Low general/tcp

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: 94479 Packet 2: 94503
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed. ... continues on next page ...

...continued from previous page...

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 the references for more information.

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

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: \$Revision: 14310 \$

References**Other:**

URL:<http://www.ietf.org/rfc/rfc1323.txt>

URL:<http://www.microsoft.com/en-us/download/details.aspx?id=9152>

[\[return to 10.0.2.4 \]](#)

Low 53/tcp

Low (CVSS: 2.6)

NVT: ISC BIND 9 DNSSEC Query Response Additional Section Remote Cache Poisoning Vulnerability

Product detection result

cpe:/a:isc:bind:9.4.2

Detected by Determine which version of BIND name daemon is running (OID: 1.3.6.1 ↪.4.1.25623.1.0.10028)

Summary

ISC BIND 9 is prone to a remote cache-poisoning vulnerability.

... continues on next page ...

...continued from previous page ...	
Vulnerability Detection Result Installed version: 9.4.2 Fixed version: 9.4.3-P4	
Impact An attacker may leverage this issue to manipulate cache data, potentially facilitating man-in-the-middle, site-impersonation, or denial-of-service attacks.	
Solution Solution type: VendorFix Updates are available. Please see the references for details.	
Affected Software/OS Versions prior to the following are vulnerable: BIND 9.4.3-P4 BIND 9.5.2-P1 BIND 9.6.1-P2	
Vulnerability Detection Method Details: ISC BIND 9 DNSSEC Query Response Additional Section Remote Cache Poisoning Vuln. ↔.. OID:1.3.6.1.4.1.25623.1.0.100362 Version used: \$Revision: 14031 \$	
Product Detection Result Product: cpe:/a:isc:bind:9.4.2 Method: Determine which version of BIND name daemon is running OID: 1.3.6.1.4.1.25623.1.0.10028)	
References CVE: CVE-2009-4022 BID:37118 Other: URL:http://www.securityfocus.com/bid/37118 URL:https://www.isc.org/node/504 URL:http://www.isc.org/products/BIND/	

[\[return to 10.0.2.4 \]](#)

Low 22/tcp

Low (CVSS: 2.1)
NVT: OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability
Product detection result cpe:/a:openbsd:openssh:4.7p1
... continues on next page ...

...continued from previous page ...
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
Summary OpenSSH is prone to a local information-disclosure vulnerability.
Vulnerability Detection Result Installed version: 4.7p1 Fixed version: 5.8p2
Impact Local attackers can exploit this issue to obtain sensitive information. Information obtained may lead to further attacks.
Solution Solution type: VendorFix 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 Checks if a vulnerable version is present on the target host. Details: OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.105002 Version used: \$Revision: 12095 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 Method: SSH Server type and version OID: 1.3.6.1.4.1.25623.1.0.10267)
References CVE: CVE-2011-4327 BID:65674 Other: URL:http://www.securityfocus.com/bid/65674 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
Product detection result cpe:/a:openbsd:openssh:4.7p1 Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
Summary OpenSSH is prone to a remote denial-of-service vulnerability.
Vulnerability Detection Result Installed version: 4.7p1 Fixed version: See references
Impact Exploiting this issue allows remote attackers to trigger denial-of-service conditions due to excessive memory consumption.
Solution Solution type: VendorFix Updates are available. Please see the references for details.
Affected Software/OS OpenSSH 5.8 and prior are vulnerable.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. 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: 14185 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 Method: SSH Server type and version OID: 1.3.6.1.4.1.25623.1.0.10267)
References CVE: CVE-2011-5000 BID:54114 Other: URL: http://www.securityfocus.com/bid/54114 URL: http://www.openssh.com
... continues on next page ...

...continued from previous page ...

Low (CVSS: 2.6) NVT: OpenSSH CBC Mode Information Disclosure Vulnerability
Product detection result cpe:/a:openbsd:openssh:4.7p1 Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
Summary The host is installed with OpenSSH and is prone to information disclosure vulnerability.
Vulnerability Detection Result Installed version: 4.7p1 Fixed version: 5.2
Impact Successful exploits will allow attackers to obtain four bytes of plaintext from an encrypted session.
Solution Solution type: VendorFix Upgrade to OpenSSH 5.2 or later.
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: 13562 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 Method: SSH Server type and version OID: 1.3.6.1.4.1.25623.1.0.10267)
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
Product detection result cpe:/a:openbsd:openssh:4.7p1 Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)
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 Installed version: 4.7p1 Fixed version: 5.7
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Affected Software/OS OpenSSH before 5.7
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: 7906 \$
Product Detection Result Product: cpe:/a:openbsd:openssh:4.7p1 Method: SSH Server type and version OID: 1.3.6.1.4.1.25623.1.0.10267)
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: 13581 \$

[\[return to 10.0.2.4 \]](#)

Low 80/tcp

Low (CVSS: 2.6) NVT: Apache 'mod_proxy_ftp' Module Denial Of Service Vulnerability (Linux)
Summary The host is running Apache 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 remote attackers to cause a Denial of Service in the context of the affected application.
Solution Solution type: VendorFix Upgrade to Apache HTTP Server version 2.2.15 or later ... continues on next page ...

...continued from previous page...
Affected Software/OS Apache HTTP Server version 2.0.x to 2.0.63 and 2.2.x to 2.2.13 on Linux.
Vulnerability Insight The flaw is due to an error in 'ap_proxy_ftp_handler' function in modules/proxy/proxy_ftp.c in the mod_proxy_ftp module while processing responses received from FTP servers. This can be exploited to trigger a NULL-pointer dereference and crash an Apache child process via a malformed EPSV response.
Vulnerability Detection Method Details: Apache 'mod_proxy_ftp' Module Denial Of Service Vulnerability (Linux) OID:1.3.6.1.4.1.25623.1.0.900841 Version used: \$Revision: 14335 \$
References CVE: CVE-2009-3094 BID:36260 Other: URL:http://intevydis.com/vd-list.shtml URL:http://www.intevydis.com/blog/?p=59 URL:http://secunia.com/advisories/36549 URL:http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html URL:http://www.apache.org/

Low (CVSS: 1.2) NVT: Apache HTTP Server 'ap_pregsub()' Function Local Denial of Service Vulnerability
Product detection result cpe:/a:apache:http_server:2.2.8 Detected by Apache Web Server Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)
Summary Apache HTTP Server is prone to a local denial-of-service vulnerability because of a NULL-pointer dereference error or a memory exhaustion.
Vulnerability Detection Result Installed version: 2.2.8 Fixed version: See references
Impact Local attackers can exploit this issue to trigger a NULL-pointer dereference or memory exhaustion, and cause a server crash, denying service to legitimate users. Note: To trigger this issue, 'mod_setenvif' must be enabled and the attacker should be able to place a malicious '.htaccess' file on the affected webserver.
... continues on next page ...

...continued from previous page ...
Solution Solution type: VendorFix
Affected Software/OS Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21 are vulnerable. Other versions may also be affected.
Vulnerability Detection Method Details: Apache HTTP Server 'ap_pregsub()' Function Local Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.103333 Version used: \$Revision: 11997 \$
Product Detection Result Product: cpe:/a:apache:http_server:2.2.8 Method: Apache Web Server Detection OID: 1.3.6.1.4.1.25623.1.0.900498)
References CVE: CVE-2011-4415 BID:50639 Other: URL:http://www.securityfocus.com/bid/50639 URL:http://httpd.apache.org/ URL:http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/ URL:http://www.gossamer-threads.com/lists/apache/dev/403775
Low (CVSS: 2.1) NVT: PHP 'mbstring.func_overload' DoS Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The host is running PHP and is prone to denial of service vulnerability.
Vulnerability Detection Result Installed version: 5.2.4 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.
... continues on next page ...

...continued from previous page ...
Solution Solution type: VendorFix Update to version 4.4.5, 5.1.7, 5.2.6 or later.
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: 14031 \$
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)
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 URL:http://php.net

Low (CVSS: 2.6) NVT: PHP display_errors Cross-Site Scripting Vulnerability
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)
Summary The host is running PHP and is prone to Cross-Site Scripting vulnerability.
Vulnerability Detection Result Installed version: 5.2.4
...continues on next page ...

...continued from previous page ...	
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.	
Solution Solution type: VendorFix Upgrade to version 5.2.8 or later.	
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: 14031 \$	
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)	
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: 1.9) NVT: PHP Security Bypass Vulnerability May18 (Linux)	
Product detection result cpe:/a:php:php:5.2.4 Detected by PHP Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)	
Summary The host is installed with php and is prone to security bypass vulnerability.	
Vulnerability Detection Result Installed version: 5.2.4 ... continues on next page ...	

...continued from previous page ...	
Fixed version:	5.6.35
Installation path / port:	80/tcp
Impact Successful exploitation will allow an attacker to bypass security restrictions and access sensitive configuration data for other accounts directly in the PHP worker process's memory.	
Solution Solution type: VendorFix Upgrade to version 7.2.4 or 7.0.29 or 5.6.35 or 7.1.16 or later. For updates refer to Reference links.	
Affected Software/OS PHP versions prior to 5.6.35, PHP versions 7.2.x prior to 7.2.4, PHP versions 7.0.x prior to 7.0.29, PHP versions 7.1.x prior to 7.1.16 on Linux.	
Vulnerability Insight The flaw exists as the dumpable FPM child processes allow bypassing opcache access controls	
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: PHP Security Bypass Vulnerability May18 (Linux) OID:1.3.6.1.4.1.25623.1.0.813162 Version used: \$Revision: 12120 \$	
Product Detection Result Product: cpe:/a:php:php:5.2.4 Method: PHP Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.800109)	
References CVE: CVE-2018-10545 Other: URL:http://www.php.net/ChangeLog-5.php#5.6.35 URL:http://www.php.net/ChangeLog-7.php#7.0.29 URL:http://www.php.net/ChangeLog-7.php#7.1.16 URL:http://www.php.net/ChangeLog-7.php#7.2.4	
Low (CVSS: 3.5) NVT: Tiki Wiki CMS Groupware XSS Vulnerability	
Product detection result cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5	
... continues on next page ...	

...continued from previous page ...
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.1.0.901001)
Summary An XSS vulnerability (via an SVG image) in Tiki allows an authenticated user to gain administrator privileges if an administrator opens a wiki page with a malicious SVG image, related to lib/filegals/filegallib.php.
Vulnerability Detection Result Installed version: 1.9.5 Fixed version: 18.0
Solution Solution type: VendorFix Upgrade to version 18.0 or later.
Affected Software/OS Tiki Wiki CMS Groupware prior to version 18.0.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: Tiki Wiki CMS Groupware XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.140797 Version used: \$Revision: 12116 \$
Product Detection Result Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Method: Tiki Wiki CMS Groupware Version Detection OID: 1.3.6.1.4.1.25623.1.0.901001)
References CVE: CVE-2018-7188 Other: URL: http://openwall.com/lists/oss-security/2018/02/16/1

[\[return to 10.0.2.4 \]](#)

Low 2121/tcp

Low (CVSS: 2.1) NVT: ProFTPD 'AllowChrootSymlinks' Local Security Bypass Vulnerability
Product detection result cpe:/a:proftpd:proftpd:1.3.1
... continues on next page ...

...continued from previous page ...
Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.↔0.900815)
Summary This host is running ProFTPD server and is prone to local security bypass vulnerability.
Vulnerability Detection Result Installed version: 1.3.1 Fixed version: 1.3.5e/1.3.6rc5
Impact Successful exploitation will allows attackers to bypass certain security restrictions and perform unauthorized actions.
Solution Solution type: VendorFix Upgrade ProFTPD 1.3.5e, 1.3.6rc5 or later.
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 Checks if a vulnerable version is present on the target host. Details: ProFTPD 'AllowChrootSymlinks' Local Security Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.810731 Version used: \$Revision: 11888 \$
Product Detection Result Product: cpe:/a:proftpd:proftpd:1.3.1 Method: ProFTPD Server Version Detection (Remote) OID: 1.3.6.1.4.1.25623.1.0.900815)
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
... continues on next page ...

...continued from previous page ...
↔821db579f URL:https://github.com/proftpd/proftpd/pull/444/commits/349addc3be4fcdad9bd4e ↔c01ad1ccd916c898ed8 URL:http://www.proftpd.org

[\[return to 10.0.2.4 \]](#)

Low 3306/tcp

Low (CVSS: 3.5) NVT: MySQL 'ALTER DATABASE' Remote Denial Of Service Vulnerability
Product detection result cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Summary The host is running MySQL 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 an attacker to cause a Denial of Service.
Solution Solution type: VendorFix Upgrade to MySQL version 5.1.48
Affected Software/OS MySQL version priot to 5.1.48 on all running platform.
Vulnerability Insight The flaw is due to an error when processing the 'ALTER DATABASE' statement and can be exploited to corrupt the MySQL data directory using the '#mysql50#' prefix followed by a '.' or '..'. NOTE: Successful exploitation requires 'ALTER' privileges on a database.
Vulnerability Detection Method Details: MySQL 'ALTER DATABASE' Remote Denial Of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.801380 Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:mysql:mysql:5.0.51a ... continues on next page ...

...continued from previous page ...
Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)
References CVE: CVE-2010-2008 BID: 41198 Other: URL: http://secunia.com/advisories/40333 URL: http://bugs.mysql.com/bug.php?id=53804 URL: http://securitytracker.com/alerts/2010/Jun/1024160.html URL: http://dev.mysql.com/doc/refman/5.1/en/news-5-1-48.html URL: http://dev.mysql.com/downloads

[\[return to 10.0.2.4 \]](#)

Low 5432/tcp

Low (CVSS: 3.5) NVT: PostgreSQL Hash Table Integer Overflow Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary The host is running PostgreSQL and is prone to integer overflow vulnerability.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: See references
Impact Successful exploitation could allow execution of specially-crafted sql query which once processed would lead to denial of service (postgresql daemon crash).
Solution Solution type: VendorFix Apply the patch linked in the references.
Affected Software/OS PostgreSQL version 8.4.1 and prior and 8.5 through 8.5alpha2
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
The flaw is due to an integer overflow error in 'src/backend/executor/nodeHash.c', when used to calculate size for the hashtable for joined relations.
Vulnerability Detection Method Details: PostgreSQL Hash Table Integer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.902139 Version used: \$Revision: 13960 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2010-0733 Other: URL:https://bugzilla.redhat.com/show_bug.cgi?id=546621 URL:http://www.openwall.com/lists/oss-security/2010/03/16/10 URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00310.php URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00289.php URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00287.php URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00277.php URL:http://git.postgresql.org/gitweb?p=postgresql.git;a=commitdiff;h=64b057e6 ↪823655fb6c5d1f24a28f236b94dd6c54

Low (CVSS: 2.1) NVT: PostgreSQL Low Cost Function Information Disclosure Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary PostgreSQL is prone to an information-disclosure vulnerability.
Vulnerability Detection Result Installed version: 8.3.1 Fixed version: See references
Impact Local attackers can exploit this issue to obtain sensitive information that may lead to further attacks.
Solution Solution type: VendorFix
... continues on next page ...

...continued from previous page ...
Updates are available. Please see the references for more information.
Affected Software/OS PostgreSQL 8.3.6 is vulnerable. Other versions may also be affected.
Vulnerability Detection Method Details: PostgreSQL Low Cost Function Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.100158 Version used: \$Revision: 14031 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References BID:34069 Other: URL:http://www.securityfocus.com/bid/34069 URL:http://www.postgresql.org/

[\[return to 10.0.2.4 \]](#)

Low 6667/tcp

Low (CVSS: 2.1) NVT: UnrealIRCd Local Privilege Escalation Vulnerability
Product detection result cpe:/a:unrealircd:unrealircd:3.2.8.1 Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)
Summary This host is installed with UnrealIRCd and is prone to local privilege escalation vulnerability.
Vulnerability Detection Result Installed version: 3.2.8.1 Fixed version: Please see the solution tag for an available Workaround
Impact Successful exploitation of this vulnerability will allow attackers to gain elevated privileges.
Solution Solution type: Workaround
... continues on next page ...

...continued from previous page ...
Please see the referenced bugreport for a workaround how to mitigate this issue within the used start scripts.
Affected Software/OS UnrealIRCd versions 4.0.13 and prior.
Vulnerability Insight The flaw exists due to error in handling of PID file. A PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a 'kill cat /pathname' command.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: UnrealIRCd Local Privilege Escalation Vulnerability OID:1.3.6.1.4.1.25623.1.0.811317 Version used: \$Revision: 11874 \$
Product Detection Result Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection OID: 1.3.6.1.4.1.25623.1.0.809884)
References CVE: CVE-2017-13649 BID:100507 Other: URL: https://vuldb.com/?id.105695 URL: http://seclists.org/oss-sec/2017/q3/343 URL: https://bugs.unrealircd.org/view.php?id=4990

[\[return to 10.0.2.4 \]](#)

Low 445/tcp

Low (CVSS: 2.1) NVT: Samba 'client/mount.cifs.c' Remote Denial of Service Vulnerability
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary Samba is prone to a remote denial-of-service vulnerability.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 3.5.11 or later Installation path / port: 445/tcp
Impact A remote attacker can exploit this issue to crash the affected application, denying service to legitimate users.
Solution Solution type: VendorFix Upgrade to Samba version 3.5.11 or later.
Affected Software/OS Samba 3.5.10 and earlier are vulnerable.
Vulnerability Detection Method Details: Samba 'client/mount.cifs.c' Remote Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.100499 Version used: \$Revision: 10398 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2010-0547, CVE-2011-2724 BID:38326 Other: URL: http://www.securityfocus.com/bid/38326 URL: http://git.samba.org/?p=samba.git;a=commit;h=a065c177dfc8f968775593ba00df↵fafaebb2e054 URL: http://us1.samba.org/samba/

Low (CVSS: 3.3) NVT: Samba 'etc/mtab' File Appending Local Denial of Service Vulnerability
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary ... continues on next page ...

...continued from previous page ...
Samba is prone to a local denial-of-service vulnerability.
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 3.5.9 Installation path / port: 445/tcp
Impact A local attacker can exploit this issue to cause the computer to stop responding, denying service to legitimate users.
Solution Solution type: VendorFix Updates are available. Please see the references for more information.
Vulnerability Detection Method Details: Samba 'etc/mtab' File Appending Local Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.103298 Version used: \$Revision: 10398 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2011-1678 BID:49939 Other: URL:http://www.securityfocus.com/bid/49939 URL:https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-1678 URL:http://us1.samba.org/samba/

Low (CVSS: 3.5) NVT: Samba Symlink Directory Traversal Vulnerability
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary Samba is prone to a directory-traversal vulnerability because the application fails to sufficiently sanitize user-supplied input.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result Installed version: 3.0.20 Fixed version: 3.3.11/3.4.6/3.5.0rc3 Installation path / port: 445/tcp
Impact Exploits would allow an attacker to access files outside of the Samba user's root directory to obtain sensitive information and perform other attacks.
Solution Solution type: VendorFix The vendor commented on the issue stating that it stems from an insecure default configuration. The Samba team advises administrators to set 'wide links = no' in the '[global]' section of 'smb.conf' and then restart the service to correct misconfigured services. Please see the references for more information.
Affected Software/OS Samba versions before 3.3.11, 3.4.x before 3.4.6, and 3.5.x before 3.5.0rc3.
Vulnerability Insight To exploit this issue, attackers require authenticated access to a writable share. Note that this issue may be exploited through a writable share accessible by guest accounts.
Vulnerability Detection Method Details: Samba Symlink Directory Traversal Vulnerability OID:1.3.6.1.4.1.25623.1.0.100488 Version used: \$Revision: 10398 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2010-0926 BID:38111 Other: URL: http://www.securityfocus.com/bid/38111 URL: http://www.samba.org/samba/news/symlink_attack.html URL: http://archives.neohapsis.com/archives/fulldisclosure/2010-02/0100.html URL: http://www.samba.org URL: http://lists.grok.org.uk/pipermail/full-disclosure/2010-February/072927.html ↪tml URL: https://www.samba.org/samba/security/CVE-2010-0926.html

[\[return to 10.0.2.4 \]](#)

Log 8787/tcp

Log (CVSS: 0.0) NVT: Service Detection with 'GET' Request
<p>Summary This plugin performs service detection. This plugin is a complement of find_service.nasl. It sends a 'GET' request to the remaining unknown services and tries to identify them.</p>
<p>Vulnerability Detection Result A Distributed Ruby (dRuby/DRb) service seems to be running on this port.</p>
<p>Log Method Details: Service Detection with 'GET' Request OID:1.3.6.1.4.1.25623.1.0.17975 Version used: \$Revision: 14067 \$</p>

[\[return to 10.0.2.4 \]](#)

Log 25/tcp

Log (CVSS: 0.0) NVT: Postfix SMTP Server Detection
<p>Summary The script checks the SMTP server banner for the presence of Postfix.</p>
<p>Vulnerability Detection Result Detected Postfix Version: unknown Location: 25/tcp CPE: cpe:/a:postfix:postfix Concluded from version/product identification result: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)</p>
<p>Log Method Details: Postfix SMTP Server Detection OID:1.3.6.1.4.1.25623.1.0.111086 Version used: \$Revision: 13461 \$</p>

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 SMTP server is running on this port Here is its banner : 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: \$Revision: 13541 \$

Log (CVSS: 0.0) NVT: SMTP Server type and version
Summary This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.
Vulnerability Detection Result Remote SMTP server banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu) The remote SMTP server is announcing the following available ESMTP commands (EHL ↪0 response) via an unencrypted connection: 8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, V ↪RFY
Log Method Details: SMTP Server type and version OID:1.3.6.1.4.1.25623.1.0.10263 Version used: \$Revision: 14004 \$

Log (CVSS: 0.0) NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection
Summary The SSL/TLS certificate on this port is self-signed.
Vulnerability Detection Result The certificate of the remote service is self signed. ... continues on next page ...

...continued from previous page ...
<p>Certificate details:</p> <pre>subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6 ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX subject alternative names (SAN): None issued by ..: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6 ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX serial: 00FAF93A4C7FB6B9CC valid from : 2010-03-17 14:07:45 UTC valid until: 2010-04-16 14:07:45 UTC fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436 ↪DE813CC</pre>
<p>Log Method</p> <p>Details: SSL/TLS: Certificate - Self-Signed Certificate Detection</p> <p>OID:1.3.6.1.4.1.25623.1.0.103140</p> <p>Version used: \$Revision: 8981 \$</p>
<p>References</p> <p>Other:</p> <p>URL:http://en.wikipedia.org/wiki/Self-signed_certificate</p>

Log (CVSS: 0.0)

NVT: SSL/TLS: Collect and Report Certificate Details

Summary

This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result

The following certificate details of the remote service were collected.

Certificate details:

```
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None
issued by ..: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
```

... continues on next page ...

...continued from previous page ...
<pre> serial: 00FAF93A4C7FB6B9CC valid from : 2010-03-17 14:07:45 UTC valid until: 2010-04-16 14:07:45 UTC fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436 ↪DE813CC </pre>
Log Method Details: SSL/TLS: Collect and Report Certificate Details OID:1.3.6.1.4.1.25623.1.0.103692 Version used: \$Revision: 13434 \$

Log (CVSS: 0.0) NVT: SSL/TLS: Report Medium Cipher Suites
Summary This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Vulnerability Detection Result 'Medium' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_DH_anon_WITH_3DES_EDE_CBC_SHA TLS_DH_anon_WITH_AES_128_CBC_SHA TLS_DH_anon_WITH_DES_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA 'Medium' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA TLS_DH_anon_WITH_3DES_EDE_CBC_SHA TLS_DH_anon_WITH_AES_128_CBC_SHA TLS_DH_anon_WITH_DES_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_DES_CBC_SHA
Vulnerability Insight Any cipher suite considered to be secure for only the next 10 years is considered as medium
Log Method Details: SSL/TLS: Report Medium Cipher Suites
... continues on next page ...

...continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.902816
 Version used: \$Revision: 4743 \$

Log (CVSS: 0.0)
 NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary

This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result

'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
 TLS_DHE_RSA_WITH_DES_CBC_SHA
 TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
 TLS_DH_anon_WITH_AES_128_CBC_SHA
 TLS_DH_anon_WITH_AES_256_CBC_SHA
 TLS_DH_anon_WITH_DES_CBC_SHA
 TLS_RSA_WITH_3DES_EDE_CBC_SHA
 TLS_RSA_WITH_AES_128_CBC_SHA
 TLS_RSA_WITH_AES_256_CBC_SHA
 TLS_RSA_WITH_DES_CBC_SHA

'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
 TLS_DHE_RSA_WITH_DES_CBC_SHA
 TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
 TLS_DH_anon_WITH_AES_128_CBC_SHA
 TLS_DH_anon_WITH_AES_256_CBC_SHA
 TLS_DH_anon_WITH_DES_CBC_SHA
 TLS_RSA_WITH_3DES_EDE_CBC_SHA
 TLS_RSA_WITH_AES_128_CBC_SHA
 TLS_RSA_WITH_AES_256_CBC_SHA
 TLS_RSA_WITH_DES_CBC_SHA

Log Method

Details: SSL/TLS: Report Non Weak Cipher Suites
 OID:1.3.6.1.4.1.25623.1.0.103441
 Version used: \$Revision: 4736 \$

Log (CVSS: 0.0)
 NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

... continues on next page ...

...continued from previous page ...
Summary This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).
Vulnerability Detection Result Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_DES_CBC_SHA
Log Method Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites OID:1.3.6.1.4.1.25623.1.0.105018 Version used: \$Revision: 4771 \$

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Supported Cipher Suites

Summary

This routine reports all SSL/TLS cipher suites accepted by a service.

As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

'Strong' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_DH_anon_WITH_AES_256_CBC_SHA

'Medium' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_DES_CBC_SHA

TLS_DH_anon_WITH_3DES_EDE_CBC_SHA

TLS_DH_anon_WITH_AES_128_CBC_SHA

TLS_DH_anon_WITH_DES_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

... continues on next page ...

...continued from previous page...

```

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
'Anonymous' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
...continues on next page ...

```

...continued from previous page...

'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol:

```
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
```

Log Method

Details: SSL/TLS: Report Supported Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.802067

Version used: \$Revision: 11108 \$

Log (CVSS: 4.3)

NVT: SSL/TLS: Report Weak Cipher Suites

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service.

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

'Weak' cipher suites accepted by this service via the SSLv3 protocol:

```
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
```

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

```
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
```

... continues on next page ...

...continued from previous page ...
TLS_RSA_WITH_RC4_128_SHA
Solution Solution type: Mitigation The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.
Vulnerability Insight These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000). - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong
Vulnerability Detection Method Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: \$Revision: 11135 \$
References CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000 Other: URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-↵1465_update_6.html URL:https://bettercrypto.org/ URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

Log (CVSS: 0.0)
NVT: SSL/TLS: SMTP 'STARTTLS' Command Detection
Summary Checks if the remote SMTP server supports SSL/TLS with the 'STARTTLS' command.
Vulnerability Detection Result The remote SMTP server supports SSL/TLS with the 'STARTTLS' command. The remote SMTP server is announcing the following available ESMTP commands (EHL ↵0 response) before sending the 'STARTTLS' command: 8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, V ↵RFY The remote SMTP server is announcing the following available ESMTP commands (EHL ↵0 response) after sending the 'STARTTLS' command: 8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, VRFY
Log Method
... continues on next page ...

...continued from previous page ...
Details: SSL/TLS: SMTP 'STARTTLS' Command Detection OID:1.3.6.1.4.1.25623.1.0.103118 Version used: \$Revision: 13822 \$
References Other: URL: https://tools.ietf.org/html/rfc3207

[\[return to 10.0.2.4 \]](#)

Log general/tcp

Log (CVSS: 0.0) NVT: OS Detection Consolidation and Reporting
<p>Summary</p> <p>This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.</p> <p>Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.</p> <p>If any of this information is wrong or could be improved please consider to report these to the referenced community portal.</p>
<p>Vulnerability Detection Result</p> <p>Best matching OS: OS: Ubuntu 8.04 Version: 8.04 CPE: cpe:/o:canonical:ubuntu_linux:8.04 Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification) Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 Setting key "Host/runs_unixoide" based on this information Other OS detections (in order of reliability): OS: Linux/Unix CPE: cpe:/o:linux:kernel Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification) Concluded from FTP banner on port 21/tcp: 220 (vsFTPD 2.3.4) OS: Debian GNU/Linux CPE: cpe:/o:debian:debian_linux Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification) Concluded from FTP banner on port 2121/tcp: 220 ProFTPD 1.3.1 Server (Debian) [:↵:ffff:10.0.2.4] OS: Debian GNU/Linux CPE: cpe:/o:debian:debian_linux Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan) Concluded from SMB/Samba banner on port 445/tcp: OS String: Debian GNU/Linux; SM↵B String: Samba 3.0.20-Debian</p>
...continues on next page ...

...continued from previous page ...

References**Other:**URL: <https://community.greenbone.net/c/vulnerability-tests>

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 172.17.0.2 to 10.0.2.4:

172.17.0.2

10.0.2.4

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: 10411 \$

[\[return to 10.0.2.4 \]](#)**Log 23/tcp**

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 telnet server seems to be running on this port

Log Method

Details: Services

OID:1.3.6.1.4.1.25623.1.0.10330

... continues on next page ...

... continued from previous page ...

Version used: \$Revision: 13541 \$

Log (CVSS: 0.0)

NVT: Telnet Banner Reporting

Summary

This scripts reports the received banner of a Telnet service.

Vulnerability Detection Result

Remote Telnet banner:

[illegible]

Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

```
metasploitable login:
```

Log Method

Details: Telnet Banner Reporting

OID:1.3.6.1.4.1.25623.1.0.10281

Version used: \$Revision: 14176 \$

Log (CVSS: 0.0)

NVT: Telnet Service Detection

Summary

This scripts tries to detect a Telnet service running at the remote host.

Vulnerability Detection Result

A Telnet server seems to be running on this port

Log Method

Details: Telnet Service Detection

OID:1.3.6.1.4.1.25623.1.0.100074

Version used: \$Revision: 13541 \$

...continues on next page ...

...continued from previous page ...

References**Other:**

URL: <https://tools.ietf.org/html/rfc854>

[\[return to 10.0.2.4 \]](#)

Log 1099/tcp

Log (CVSS: 0.0)

NVT: RMI-Registry Detection

Summary

This Script detects the RMI-Registry Service

Vulnerability Detection Result

The RMI-Registry Service is running at this port

Log Method

Details: RMI-Registry Detection

OID:1.3.6.1.4.1.25623.1.0.105839

Version used: \$Revision: 13541 \$

[\[return to 10.0.2.4 \]](#)

Log 3632/tcp

Log (CVSS: 0.0)

NVT: DistCC Detection

Summary

Tries to detect if the remote host is running a DistCC service.

Vulnerability Detection Result

A DistCC service is running at this port.

Log Method

Details: DistCC Detection

OID:1.3.6.1.4.1.25623.1.0.12638

Version used: \$Revision: 13541 \$

[\[return to 10.0.2.4 \]](#)

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.
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: 10411 \$
References CVE: CVE-1999-0524 Other: URL: http://www.ietf.org/rfc/rfc0792.txt

[\[return to 10.0.2.4 \]](#)

Log 21/tcp

Log (CVSS: 0.0) NVT: FTP Banner Detection
Summary This Plugin detects and reports a FTP Server Banner.
Vulnerability Detection Result Remote FTP server banner: 220 (vsFTPd 2.3.4) This is probably: - vsFTPd Server operating system information collected via "SYST" command: 215 UNIX Type: L8 Server status information collected via "STAT" command: 211-FTP server status: Connected to 10.0.2.15 Logged in as ftp ... continues on next page ...

...continued from previous page ...
TYPE: ASCII No session bandwidth limit Session timeout in seconds is 300 Control connection is plain text Data connections will be plain text vsFTPD 2.3.4 - secure, fast, stable 211 End of status
Log Method Details: FTP Banner Detection OID:1.3.6.1.4.1.25623.1.0.10092 Version used: \$Revision: 13637 \$

Log (CVSS: 0.0) NVT: FTP Missing Support For AUTH TLS
Summary The remote FTP server does not support the 'AUTH TLS' command.
Vulnerability Detection Result The remote FTP server does not support the 'AUTH TLS' command.
Log Method Details: FTP Missing Support For AUTH TLS OID:1.3.6.1.4.1.25623.1.0.108553 Version used: \$Revision: 13863 \$

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 FTP server is running on this port. Here is its banner : 220 (vsFTPD 2.3.4)
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: \$Revision: 13541 \$

Log (CVSS: 0.0) NVT: vsFTPd FTP Server Detection
Summary The script is grabbing the banner of a FTP server and attempts to identify a vsFTPd FTP Server and its version from the reply.
Vulnerability Detection Result Detected vsFTPd Version: 2.3.4 Location: 21/tcp CPE: cpe:/a:beasts:vsftpd:2.3.4 Concluded from version/product identification result: 220 (vsFTPd 2.3.4)
Log Method Details: vsFTPd FTP Server Detection OID:1.3.6.1.4.1.25623.1.0.111050 Version used: \$Revision: 13499 \$

[\[return to 10.0.2.4 \]](#)

Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.
Vulnerability Detection Result 10.0.2.4 cpe:/a:apache:http_server:2.2.8 10.0.2.4 cpe:/a:beasts:vsftpd:2.3.4 10.0.2.4 cpe:/a:isc:bind:9.4.2 10.0.2.4 cpe:/a:jquery:jquery 10.0.2.4 cpe:/a:mysql:mysql:5.0.51a 10.0.2.4 cpe:/a:openbsd:openssh:4.7p1 10.0.2.4 cpe:/a:php:php:5.2.4 10.0.2.4 cpe:/a:phpmyadmin:phpmyadmin:3.1.1 10.0.2.4 cpe:/a:postfix:postfix 10.0.2.4 cpe:/a:postgresql:postgresql:8.3.1 10.0.2.4 cpe:/a:proftpd:proftpd:1.3.1 10.0.2.4 cpe:/a:samba:samba:3.0.20 10.0.2.4 cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 10.0.2.4 cpe:/a:twiki:twiki:01.Feb.2003 10.0.2.4 cpe:/a:unrealircd:unrealircd:3.2.8.1 ... continues on next page ...

...continued from previous page ...	
10.0.2.4 cpe:/a:x.org:x11:11.0	
10.0.2.4 cpe:/o:canonical:ubuntu_linux:8.04	
Log Method Details: CPE Inventory OID:1.3.6.1.4.1.25623.1.0.810002 Version used: \$Revision: 14324 \$	
References Other: URL:http://cpe.mitre.org/	

[\[return to 10.0.2.4 \]](#)

Log 512/tcp

Log (CVSS: 0.0) NVT: Service Detection with 'BINARY' Request	
Summary This plugin performs service detection. This plugin is a complement of find_service.nasl. It sends a 'BINARY' request to the remaining unknown services and tries to identify them.	
Vulnerability Detection Result A rexec service seems to be running on this port.	
Log Method Details: Service Detection with 'BINARY' Request OID:1.3.6.1.4.1.25623.1.0.108204 Version used: \$Revision: 14246 \$	

[\[return to 10.0.2.4 \]](#)

Log 111/tcp

Log (CVSS: 0.0) NVT: Obtain list of all port mapper registered programs via RPC	
Summary This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.	
Vulnerability Detection Result These are the registered RPC programs:	
... continues on next page ...	

...continued from previous page...
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/ ↔TCP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/TCP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/TCP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/TCP
RPC program #100021 version 1 'nlockmgr' on port 37792/TCP
RPC program #100021 version 3 'nlockmgr' on port 37792/TCP
RPC program #100021 version 4 'nlockmgr' on port 37792/TCP
RPC program #100024 version 1 'status' on port 52148/TCP
RPC program #100005 version 1 'mountd' (mount showmount) on port 56592/TCP
RPC program #100005 version 2 'mountd' (mount showmount) on port 56592/TCP
RPC program #100005 version 3 'mountd' (mount showmount) on port 56592/TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/ ↔UDP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/UDP
RPC program #100024 version 1 'status' on port 33878/UDP
RPC program #100005 version 1 'mountd' (mount showmount) on port 34083/UDP
RPC program #100005 version 2 'mountd' (mount showmount) on port 34083/UDP
RPC program #100005 version 3 'mountd' (mount showmount) on port 34083/UDP
RPC program #100021 version 1 'nlockmgr' on port 44087/UDP
RPC program #100021 version 3 'nlockmgr' on port 44087/UDP
RPC program #100021 version 4 'nlockmgr' on port 44087/UDP
Log Method Details: Obtain list of all port mapper registered programs via RPC OID:1.3.6.1.4.1.25623.1.0.11111 Version used: \$Revision: 13541 \$

Log (CVSS: 0.0) NVT: RPC portmapper (TCP)
Summary This script performs detection of RPC portmapper on TCP.
Vulnerability Detection Result RPC portmapper is running on this port.
Log Method Details: RPC portmapper (TCP) OID:1.3.6.1.4.1.25623.1.0.108090 Version used: \$Revision: 13541 \$

[\[return to 10.0.2.4 \]](#)

Log 514/tcp

Log (CVSS: 0.0) NVT: rsh Service Detection
Summary Checks if the remote host is running a rsh service. Note: The reporting takes place in a separate VT 'rsh Unencrypted Cleartext Login' (OID: 1.3.6.1.4.1.25623.1.0.100080).
Vulnerability Detection Result A rsh service is running at this port.
Log Method Details: rsh Service Detection OID:1.3.6.1.4.1.25623.1.0.108478 Version used: \$Revision: 13541 \$

[\[return to 10.0.2.4 \]](#)

Log 53/tcp

Log (CVSS: 0.0) NVT: Determine which version of BIND name daemon is running
Summary BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code.
Vulnerability Detection Result Detected Bind Version: 9.4.2 Location: 53/tcp CPE: cpe:/a:isc:bind:9.4.2 Concluded from version/product identification result: 9.4.2
Solution Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts.
Vulnerability Insight The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source.
... continues on next page ...

...continued from previous page...

Log Method

Details: Determine which version of BIND name daemon is running

OID:1.3.6.1.4.1.25623.1.0.10028

Version used: \$Revision: 10945 \$

Log (CVSS: 0.0)

NVT: DNS Server Detection (TCP)

Summary

A DNS Server is running at this Host. A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address.

Vulnerability Detection Result

The remote DNS server banner is:
9.4.2

Log Method

Details: DNS Server Detection (TCP)

OID:1.3.6.1.4.1.25623.1.0.108018

Version used: \$Revision: 13541 \$

[\[return to 10.0.2.4 \]](#)**Log 139/tcp**

Log (CVSS: 0.0)

NVT: SMB/CIFS Server Detection

Summary

This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result

A SMB server is running on this port

Log Method

Details: SMB/CIFS Server Detection

OID:1.3.6.1.4.1.25623.1.0.11011

Version used: \$Revision: 13541 \$

[\[return to 10.0.2.4 \]](#)**Log 22/tcp**

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: 13541 \$

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-hellman-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,aes192-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,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr mac_algorithms_client_to_server: hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96 mac_algorithms_server_to_client: hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96 compression_algorithms_client_to_server: none,zlib@openssh.com compression_algorithms_server_to_client: none,zlib@openssh.com
Log Method ... continues on next page ...

...continued from previous page ...

Details: SSH Protocol Algorithms Supported
 OID:1.3.6.1.4.1.25623.1.0.105565
 Version used: \$Revision: 13581 \$

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

2.0

SSHv2 Fingerprint(s):

ssh-dss: 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd

ssh-rsa: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3

Log Method

Details: SSH Protocol Versions Supported

OID:1.3.6.1.4.1.25623.1.0.100259

Version used: \$Revision: 13594 \$

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

Remote SSH server banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

Remote SSH supported authentication: password,publickey

Remote SSH text/login banner: (not available)

This is probably:

- OpenSSH

CPE: cpe:/a:openbsd:openssh:4.7p1

Concluded from remote connection attempt with credentials:

Login: OpenVAS-VT

Password: OpenVAS-VT

... continues on next page ...

...continued from previous page ...

Log Method

Details: SSH Server type and version

OID:1.3.6.1.4.1.25623.1.0.10267

Version used: 2019-03-22T07:02:59+0000

[\[return to 10.0.2.4 \]](#)**Log 6000/tcp**

Log (CVSS: 0.0)

NVT: X Server Detection

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: 6000/tcp

CPE: cpe:/a:x.org:x11:11.0

Concluded from version/product identification result:

11.0

Extra information:

Server answered with: Client is not authorized

Log Method

Details: X Server Detection

OID:1.3.6.1.4.1.25623.1.0.10407

Version used: \$Revision: 10123 \$

[\[return to 10.0.2.4 \]](#)**Log 80/tcp**

Log (CVSS: 0.0)

NVT: Apache Web Server Detection

... continues on next page ...

...continued from previous page ...
Summary Detects the 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: 2.2.8 Location: 80/tcp CPE: cpe:/a:apache:http_server:2.2.8 Concluded from version/product identification result: Server: Apache/2.2.8
Log Method Details: Apache Web Server Detection OID:1.3.6.1.4.1.25623.1.0.900498 Version used: \$Revision: 10290 \$

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:

- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- 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
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

The Hostname/IP "10.0.2.4" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

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 User-Agent "Mozilla/5.0 [en] (X11; U; OpenVAS-VT 9.0.3)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

... continues on next page ...

...continued from previous page ...

The following directories were used for CGI scanning:

```
http://10.0.2.4/
http://10.0.2.4/cgi-bin
http://10.0.2.4/dav
http://10.0.2.4/doc
http://10.0.2.4/dvwa
http://10.0.2.4/mutillidae
http://10.0.2.4/mutillidae/documentation
http://10.0.2.4/oops/TWiki
http://10.0.2.4/phpMyAdmin
http://10.0.2.4/rdiff/TWiki
http://10.0.2.4/test
http://10.0.2.4/test/testoutput
http://10.0.2.4/tikiwiki
http://10.0.2.4/tikiwiki/lib
http://10.0.2.4/twiki
http://10.0.2.4/twiki/pub/TWiki/TWikiDocGraphics
http://10.0.2.4/twiki/pub/TWiki/TWikiLogos
http://10.0.2.4/view/TWiki
```

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index|php|image|img|css|js|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media|skins?)/"

```
http://10.0.2.4/icons
http://10.0.2.4/mutillidae/images
http://10.0.2.4/mutillidae/javascript
http://10.0.2.4/mutillidae/javascript/ddsmoothmenu
http://10.0.2.4/mutillidae/styles
http://10.0.2.4/mutillidae/styles/ddsmoothmenu
http://10.0.2.4/phpMyAdmin/themes/original/img
http://10.0.2.4/tikiwiki/img/icons
http://10.0.2.4/tikiwiki/styles
http://10.0.2.4/tikiwiki/styles/transitions
```

Directory index found at:

```
http://10.0.2.4/dav/
http://10.0.2.4/test/
http://10.0.2.4/test/testoutput/
http://10.0.2.4/twiki/TWikiDocumentation.html
```

Extraneous phpinfo() script found at:

```
http://10.0.2.4/mutillidae/phpinfo.php
http://10.0.2.4/phpinfo.php
```

PHP script discloses physical path at:

```
http://10.0.2.4/tikiwiki/tiki-install.php (/var/www/tikiwiki/lib/adodb/drivers/a
```

...continues on next page ...

...continued from previous page...

```

↪dodb-mysql.inc.php)
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://10.0.2.4/dav/ (C=S;0 [A] C=N;0 [D] C=M;0 [A] C=D;0 [A] )
http://10.0.2.4/mutillidae/ (page [add-to-your-blog.php] )
http://10.0.2.4/mutillidae/documentation/ (C=S;0 [A] C=N;0 [D] C=M;0 [A] C=D;0 [
↪A] )
http://10.0.2.4/mutillidae/index.php (username [anonymous] do [toggle-hints] pag
↪e [home.php] )
http://10.0.2.4/oops/TWiki/TWikiHistory (template [oopsrev] param1 [1.10] )
http://10.0.2.4/phpMyAdmin/index.php (phpMyAdmin [0e29078e7ac43257dac4f627e9092f
↪aeab35b5a7] token [86bdee2c065ec1e18a99a6eb6d09d537] pma_username [] table []
↪lang [] server [1] db [] convcharset [utf-8] pma_password [] )
http://10.0.2.4/phpMyAdmin/phpmyadmin.css.php (token [86bdee2c065ec1e18a99a6eb6d
↪09d537] js_frame [right] lang [en-utf-8] nocache [2457687151] convcharset [utf
↪-8] )
http://10.0.2.4/rdiff/TWiki/TWikiHistory (rev1 [1.10] rev2 [1.9] )
http://10.0.2.4/test/ (C=S;0 [A] C=N;0 [D] C=M;0 [A] C=D;0 [A] )
http://10.0.2.4/test/testoutput/ (C=S;0 [A] C=N;0 [D] C=M;0 [A] C=D;0 [A] )
http://10.0.2.4/tikiwiki/tiki-install.php (host [localhost] dbinfo [] pass [] na
↪me [] db [] restart [1] resetdb [] user [] )
http://10.0.2.4/twiki/bin/edit/Know/WebHome (t [1709064956] )
http://10.0.2.4/twiki/bin/edit/Main/EngineeringGroup (topicparent [Main.TWikiGro
↪ups] )
http://10.0.2.4/twiki/bin/edit/Main/OfficeLocations (t [1709065006] )
http://10.0.2.4/twiki/bin/edit/Main/SupportGroup (topicparent [Main.TWikiGroups]
↪ )
http://10.0.2.4/twiki/bin/edit/Main/TWikiGroups (t [1709064997] )
http://10.0.2.4/twiki/bin/edit/Main/TWikiUsers (t [1709064988] )
http://10.0.2.4/twiki/bin/edit/Main/WebChanges (t [1709065015] )
http://10.0.2.4/twiki/bin/edit/Main/WebHome (t [1709064882] )
http://10.0.2.4/twiki/bin/edit/Main/WebIndex (t [1709065046] )
http://10.0.2.4/twiki/bin/edit/Main/WebSearch (t [1709065052] )
http://10.0.2.4/twiki/bin/edit/Main/WebTopicEditTemplate (topicparent [Main.WebP
↪references] )
http://10.0.2.4/twiki/bin/edit/Sandbox/TestTopic1 (topicparent [Sandbox.WebHome]
↪ )
http://10.0.2.4/twiki/bin/edit/Sandbox/TestTopic2 (topicparent [Sandbox.WebHome]
↪ )
http://10.0.2.4/twiki/bin/edit/Sandbox/TestTopic3 (topicparent [Sandbox.WebHome]
↪ )
http://10.0.2.4/twiki/bin/edit/Sandbox/TestTopic4 (topicparent [Sandbox.WebHome]
↪ )
http://10.0.2.4/twiki/bin/edit/Sandbox/TestTopic5 (topicparent [Sandbox.WebHome]
↪ )
http://10.0.2.4/twiki/bin/edit/Sandbox/TestTopic6 (topicparent [Sandbox.WebHome]
↪ )

```

...continues on next page...

...continued from previous page...	
http://10.0.2.4/twiki/bin/edit/Sandbox/TestTopic7 (topicparent [Sandbox.WebHome]	
↔)	
http://10.0.2.4/twiki/bin/edit/Sandbox/TestTopic8 (topicparent [Sandbox.WebHome]	
↔)	
http://10.0.2.4/twiki/bin/edit/Sandbox/WebHome (t [1709064967])	
http://10.0.2.4/twiki/bin/edit/TWiki/WebHome (t [1709064916])	
http://10.0.2.4/twiki/bin/oops/Know/WebHome (template [oopsmore] param1 [1.10] p	
↔aram2 [1.10])	
http://10.0.2.4/twiki/bin/oops/Main/OfficeLocations (template [oopsmore] param1	
↔[1.4] param2 [1.4])	
http://10.0.2.4/twiki/bin/oops/Main/TWikiGroups (template [oopsmore] param1 [1.3	
↔] param2 [1.3])	
http://10.0.2.4/twiki/bin/oops/Main/TWikiUsers (template [oopsmore] param1 [1.16	
↔] param2 [1.16])	
http://10.0.2.4/twiki/bin/oops/Main/WebChanges (template [oopsmore] param1 [1.2]	
↔ param2 [1.2])	
http://10.0.2.4/twiki/bin/oops/Main/WebHome (template [oopsmore] param1 [1.20] p	
↔aram2 [1.20])	
http://10.0.2.4/twiki/bin/oops/Main/WebIndex (template [oopsmore] param1 [1.2] p	
↔aram2 [1.2])	
http://10.0.2.4/twiki/bin/oops/Main/WebSearch (template [oopsmore] param1 [1.8]	
↔param2 [1.8])	
http://10.0.2.4/twiki/bin/oops/Sandbox/WebHome (template [oopsmore] param1 [1.7]	
↔ param2 [1.7])	
http://10.0.2.4/twiki/bin/oops/TWiki/WebHome (template [oopsmore] param1 [1.78]	
↔param2 [1.78])	
http://10.0.2.4/twiki/bin/rdiff/Know/WebHome (rev1 [1.10] rev2 [1.9])	
http://10.0.2.4/twiki/bin/rdiff/Main/OfficeLocations (rev1 [1.4] rev2 [1.3])	
http://10.0.2.4/twiki/bin/rdiff/Main/TWikiGroups (rev1 [1.3] rev2 [1.2])	
http://10.0.2.4/twiki/bin/rdiff/Main/TWikiUsers (rev1 [1.16] rev2 [1.15])	
http://10.0.2.4/twiki/bin/rdiff/Main/WebChanges (rev1 [1.2] rev2 [1.1])	
http://10.0.2.4/twiki/bin/rdiff/Main/WebHome (rev1 [1.20] rev2 [1.19])	
http://10.0.2.4/twiki/bin/rdiff/Main/WebIndex (rev1 [1.2] rev2 [1.1])	
http://10.0.2.4/twiki/bin/rdiff/Main/WebSearch (rev1 [1.8] rev2 [1.7])	
http://10.0.2.4/twiki/bin/rdiff/Sandbox/WebHome (rev1 [1.7] rev2 [1.6])	
http://10.0.2.4/twiki/bin/rdiff/TWiki/WebHome (rev1 [1.78] rev2 [1.77])	
http://10.0.2.4/twiki/bin/search/Know/SearchResult (search [] scope [text] regex	
↔ [on])	
http://10.0.2.4/twiki/bin/search/Main/ (showlock [] search [%5C.*] web [] scope	
↔[topic] nosearch [on] reverse [on] regex [on] order [modified] limit [100] not	
↔otal [] bookview [] nosummary [] casesensitive [])	
http://10.0.2.4/twiki/bin/search/Main/SearchResult (search [] scope [text] nosea	
↔rch [on] reverse [on] regex [on] order [modified])	
http://10.0.2.4/twiki/bin/search/Sandbox/SearchResult (search [] scope [text] re	
↔gex [on])	
http://10.0.2.4/twiki/bin/search/TWiki/ (search [])	
http://10.0.2.4/twiki/bin/search/TWiki/SearchResult (search [] scope [text] rege	
...continues on next page...	

...continued from previous page...
<pre> ↪x [on]) http://10.0.2.4/twiki/bin/view/Know/WebHome (topic [] skin [print] rev [1.9]) http://10.0.2.4/twiki/bin/view/Main/OfficeLocations (topic [] skin [print] rev [↪1.3]) http://10.0.2.4/twiki/bin/view/Main/TWikiGroups (topic [] skin [print] rev [1.2] ↪) http://10.0.2.4/twiki/bin/view/Main/TWikiUsers (topic [] skin [print] rev [1.15] ↪) http://10.0.2.4/twiki/bin/view/Main/WebChanges (topic [] skin [print] rev [1.1] ↪) http://10.0.2.4/twiki/bin/view/Main/WebHome (topic [] skin [print] rev [1.19]) http://10.0.2.4/twiki/bin/view/Main/WebIndex (topic [] skin [print] rev [1.1]) http://10.0.2.4/twiki/bin/view/Main/WebPreferences (topic []) http://10.0.2.4/twiki/bin/view/Main/WebSearch (topic [] skin [print] rev [1.7]) http://10.0.2.4/twiki/bin/view/Sandbox/WebHome (topic [] skin [print] rev [1.6] ↪) http://10.0.2.4/twiki/bin/view/TWiki/WebHome (topic [] skin [print] rev [1.77]) http://10.0.2.4/view/TWiki/TWikiHistory (rev [1.9]) </pre>
Log Method Details: CGI Scanning Consolidation OID:1.3.6.1.4.1.25623.1.0.111038 Version used: \$Revision: 13679 \$
References Other: URL: https://community.greenbone.net/c/vulnerability-tests

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: "phpmyadmin (2.11.8.1 - 4.2.x)" fingerprinted by the file: "http://10.0.2.4/phpM ↪yAdmin/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.
Solution Solution type: Mitigation Remove the 'favicon.ico' file or create a custom one for your site.
... continues on next page ...

...continued from previous page ...

Log Method

Details: Fingerprint web server with favicon.ico

OID:1.3.6.1.4.1.25623.1.0.20108

Version used: \$Revision: 11730 \$

Log (CVSS: 0.0)

NVT: HTTP Security Headers Detection

Summary

All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result

Missing Headers

Content-Security-Policy

Referrer-Policy

X-Content-Type-Options

X-Frame-Options

X-Permitted-Cross-Domain-Policies

X-XSS-Protection

Log Method

Details: HTTP Security Headers Detection

OID:1.3.6.1.4.1.25623.1.0.112081

Version used: \$Revision: 10899 \$

References

Other:

URL:https://www.owasp.org/index.php/OWASP_Secure-Headers_ProjectURL:https://www.owasp.org/index.php/OWASP_Secure-Headers_Project#tab=HeadersURL:<https://securityheaders.io/>

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/2.2.8 (Ubuntu) DAV/2

Solution : You can set the directive "ServerTokens Prod" to limit

... continues on next page ...

...continued from previous page ...
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: 11585 \$

Log (CVSS: 0.0) NVT: jQuery Detection
Summary Detection of jQuery. The script sends a connection request to the server and attempts to detect jQuery and to extract its version.
Vulnerability Detection Result Detected jQuery Version: unknown Location: /mutillidae/javascript/ddsmoothmenu CPE: cpe:/a:jquery:jquery
Log Method Details: jQuery Detection OID:1.3.6.1.4.1.25623.1.0.141622 Version used: \$Revision: 14001 \$
References Other: URL:https://jquery.com/

Log (CVSS: 0.0) NVT: PHP Version Detection (Remote)
Summary Detects the 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 Detected PHP
... continues on next page ...

...continued from previous page ...

Version: 5.2.4
Location: 80/tcp
CPE: cpe:/a:php:php:5.2.4
Concluded from version/product identification result:
X-Powered-By: PHP/5.2.4-2ubuntu5.10

Log Method

Details: PHP Version Detection (Remote)
OID:1.3.6.1.4.1.25623.1.0.800109
Version used: \$Revision: 13811 \$

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: 3.1.1
Location: /phpMyAdmin
CPE: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Concluded from version/product identification result:
Version 3.1.1
Concluded from version/product identification location:
http://10.0.2.4/phpMyAdmin/README
Extra information:
- Protected by Username/Password

Log Method

Details: phpMyAdmin Detection
OID:1.3.6.1.4.1.25623.1.0.900129
Version used: \$Revision: 12754 \$

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

... continues on next page ...

...continued from previous page ...
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: 13541 \$

Log (CVSS: 0.0) NVT: Tiki Wiki CMS Groupware Version Detection
Summary Detection of Tiki Wiki CMS Groupware, a open source web application is a wiki-based CMS. The script sends a connection request to the web server and attempts to extract the version number from the reply.
Vulnerability Detection Result Detected Tiki Wiki CMS Groupware Version: 1.9.5 Location: /tikiwiki CPE: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Concluded from version/product identification result: version 1.9.5 Concluded from version/product identification location: http://10.0.2.4/tikiwiki/README
Log Method Details: Tiki Wiki CMS Groupware Version Detection OID:1.3.6.1.4.1.25623.1.0.901001 Version used: \$Revision: 10894 \$
References Other: URL:http://tiki.org/

Log (CVSS: 0.0) NVT: TWiki Version Detection
Summary Detection of TWiki. The script sends a HTTP connection request to the server and attempts to detect the presence of TWiki and to extract its version.
Vulnerability Detection Result Detected TWiki Version: 01.Feb.2003
... continues on next page ...

...continued from previous page ...
Location: /twiki/bin CPE: cpe:/a:twiki:twiki:01.Feb.2003 Concluded from version/product identification result: This site is running Twiki version 01 Feb 2003
Log Method Details: TWiki Version Detection OID:1.3.6.1.4.1.25623.1.0.800399 Version used: \$Revision: 12952 \$

Log (CVSS: 0.0) NVT: wapiti (NASL wrapper)
Summary This plugin uses wapiti to find web security issues. Make sure to have wapiti 2.x as wapiti 1.x is not supported. See the preferences section for wapiti options. Note that the scanner is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks. Note: The plugin needs the 'wapiti' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).
Vulnerability Detection Result The wapiti report filename is empty. That could mean that a wrong version of wapiti is used or tmp dir is not accessible. Make sure to have wapiti 2.x as wapiti 1.x is not supported. In short: Check the installation of wapiti and the scanner.
Log Method Details: wapiti (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.80110 Version used: \$Revision: 13985 \$

[\[return to 10.0.2.4 \]](#)

Log 2121/tcp

Log (CVSS: 0.0) NVT: FTP Banner Detection
Summary This Plugin detects and reports a FTP Server Banner.
Vulnerability Detection Result ... continues on next page ...

...continued from previous page...

Remote FTP server banner:
 220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.0.2.4]
 This is probably:
 - ProFTPD
 Server operating system information collected via "SYST" command:
 215 UNIX Type: L8

Log Method

Details: FTP Banner Detection
 OID:1.3.6.1.4.1.25623.1.0.10092
 Version used: \$Revision: 13637 \$

Log (CVSS: 0.0)

NVT: FTP Missing Support For AUTH TLS

Summary

The remote FTP server does not support the 'AUTH TLS' command.

Vulnerability Detection Result

The remote FTP server does not support the 'AUTH TLS' command.

Log Method

Details: FTP Missing Support For AUTH TLS
 OID:1.3.6.1.4.1.25623.1.0.108553
 Version used: \$Revision: 13863 \$

Log (CVSS: 0.0)

NVT: ProFTPD Server Version Detection (Remote)

Summary

This script detects the installed version of ProFTP Server and sets the version in KB.

Vulnerability Detection Result

Detected ProFTPD
 Version: 1.3.1
 Location: 2121/tcp
 CPE: cpe:/a:proftpd:proftpd:1.3.1
 Concluded from version/product identification result:
 220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.0.2.4]

Log Method

Details: ProFTPD Server Version Detection (Remote)
 OID:1.3.6.1.4.1.25623.1.0.900815
 Version used: \$Revision: 13499 \$

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 FTP server is running on this port. Here is its banner : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.0.2.4]
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: \$Revision: 13541 \$

[\[return to 10.0.2.4 \]](#)

Log 3306/tcp

Log (CVSS: 0.0) NVT: Database Open Access Vulnerability
Summary The host is running a Database server and is prone to information disclosure vulnerability.
Vulnerability Detection Result MySQL can be accessed by remote attackers
Impact Successful exploitation could allow an attacker to obtain the sensitive information of the database.
Solution Solution type: Workaround Restrict Database access to remote systems.
Affected Software/OS - MySQL/MariaDB - IBM DB2 - PostgreSQL - IBM solidDB - Oracle Database - Microsoft SQL Server
Vulnerability Insight ... continues on next page ...

...continued from previous page ...
Do not restricting direct access of databases to the remote systems.
Log Method Details: Database Open Access Vulnerability OID:1.3.6.1.4.1.25623.1.0.902799 Version used: \$Revision: 11374 \$
References Other: URL: https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_d↵ss_v1-2.pdf

Log (CVSS: 0.0) NVT: MySQL/MariaDB Detection
Summary Detects the installed version of MySQL/MariaDB. 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: 5.0.51a-3ubuntu5 Location: 3306/tcp CPE: cpe:/a:mysql:mysql:5.0.51a Concluded from version/product identification result: 5.0.51a-3ubuntu5
Log Method Details: MySQL/MariaDB Detection OID:1.3.6.1.4.1.25623.1.0.100152 Version used: \$Revision: 10929 \$

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 unknown service is running on this port. It is usually reserved for MySQL
... continues on next page ...

...continued from previous page ...

Log MethodDetails: **Services**

OID:1.3.6.1.4.1.25623.1.0.10330

Version used: \$Revision: 13541 \$

[\[return to 10.0.2.4 \]](#)**Log 1524/tcp**

Log (CVSS: 0.0)

NVT: Service Detection with 'GET' Request

Summary

This plugin performs service detection.

This plugin is a complement of find_service.nasl. It sends a 'GET' request to the remaining unknown services and tries to identify them.

Vulnerability Detection Result

A root shell of Metasploitable seems to be running on this port.

Log Method

Details: Service Detection with 'GET' Request

OID:1.3.6.1.4.1.25623.1.0.17975

Version used: \$Revision: 14067 \$

[\[return to 10.0.2.4 \]](#)**Log 5432/tcp**

Log (CVSS: 0.0)

NVT: Database Open Access Vulnerability

Summary

The host is running a Database server and is prone to information disclosure vulnerability.

Vulnerability Detection Result

PostgreSQL database can be accessed by remote attackers

Impact

Successful exploitation could allow an attacker to obtain the sensitive information of the database.

Solution**Solution type:** Workaround

Restrict Database access to remote systems.

... continues on next page ...

...continued from previous page ...

Affected Software/OS

- MySQL/MariaDB
- IBM DB2
- PostgreSQL
- IBM solidDB
- Oracle Database
- Microsoft SQL Server

Vulnerability Insight

Do not restricting direct access of databases to the remote systems.

Log Method

Details: Database Open Access Vulnerability

OID:1.3.6.1.4.1.25623.1.0.902799

Version used: \$Revision: 11374 \$

References

Other:

URL:https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_d↵ss_v1-2.pdf

Log (CVSS: 0.0)

NVT: PostgreSQL Detection

Summary

Detection of PostgreSQL, a open source object-relational database system.

The script sends a connection request to the server (user:postgres, DB:postgres) and attempts to extract the version number from the reply.

Vulnerability Detection Result

Detected PostgreSQL

Version: 8.3.1

Location: 5432/tcp

CPE: cpe:/a:postgresql:postgresql:8.3.1

Concluded from version/product identification result:
8.3.1

Log Method

Details: PostgreSQL Detection

OID:1.3.6.1.4.1.25623.1.0.100151

Version used: \$Revision: 14324 \$

References

Other:

URL:<http://http://www.postgresql.org>

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 unknown service is running on this port. It is usually reserved for Postgres
Log Method Details: Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: \$Revision: 13541 \$

Log (CVSS: 0.0) NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection
Summary The SSL/TLS certificate on this port is self-signed.
Vulnerability Detection Result The certificate of the remote service is self signed. Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6 ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6 ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX serial: 00FAF93A4C7FB6B9CC valid from : 2010-03-17 14:07:45 UTC valid until: 2010-04-16 14:07:45 UTC fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436 ↪DE813CC
Log Method Details: SSL/TLS: Certificate - Self-Signed Certificate Detection OID:1.3.6.1.4.1.25623.1.0.103140 Version used: \$Revision: 8981 \$
... continues on next page ...

...continued from previous page ...

References**Other:**URL:http://en.wikipedia.org/wiki/Self-signed_certificate

Log (CVSS: 0.0)

NVT: SSL/TLS: Collect and Report Certificate Details

Summary

This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result

The following certificate details of the remote service were collected.

Certificate details:

```
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
```

subject alternative names (SAN):

None

```
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
```

```
serial ....: 00FAF93A4C7FB6B9CC
```

```
valid from : 2010-03-17 14:07:45 UTC
```

```
valid until: 2010-04-16 14:07:45 UTC
```

```
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
```

```
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Log Method

Details: SSL/TLS: Collect and Report Certificate Details

OID:1.3.6.1.4.1.25623.1.0.103692

Version used: \$Revision: 13434 \$

Log (CVSS: 0.0)

NVT: SSL/TLS: PostgreSQL SSL/TLS Support Detection

Summary

Checks if the remote PostgreSQL server supports SSL/TLS.

Vulnerability Detection Result

The remote PostgreSQL server supports SSL/TLS.

... continues on next page ...

...continued from previous page ...

Log Method

Details: SSL/TLS: PostgreSQL SSL/TLS Support Detection

OID:1.3.6.1.4.1.25623.1.0.105013

Version used: \$Revision: 11915 \$

References

Other:

URL:<https://www.postgresql.org/docs/current/static/ssl-tcp.html>

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Medium Cipher Suites

Summary

This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result

'Medium' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

Vulnerability Insight

Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method

Details: SSL/TLS: Report Medium Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.902816

Version used: \$Revision: 4743 \$

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary

This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result

... continues on next page ...

...continued from previous page...

'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

Log Method

Details: SSL/TLS: Report Non Weak Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.103441

Version used: \$Revision: 4736 \$

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Summary

This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Vulnerability Detection Result

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Log Method

Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.105018

Version used: \$Revision: 4771 \$

Log (CVSS: 0.0)

NVT: SSL/TLS: Report Supported Cipher Suites

Summary

This routine reports all SSL/TLS cipher suites accepted by a service.

As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

'Strong' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

'Medium' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

'Weak' cipher suites accepted by this service via the SSLv3 protocol:

TLS_RSA_WITH_RC4_128_SHA

No 'Null' cipher suites accepted by this service via the SSLv3 protocol.

No 'Anonymous' cipher suites accepted by this service via the SSLv3 protocol.

'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_RC4_128_SHA

No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.

Log Method

Details: SSL/TLS: Report Supported Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.802067

Version used: \$Revision: 11108 \$

[\[return to 10.0.2.4 \]](#)

Log 6667/tcp

Log (CVSS: 0.0) NVT: IRC Server Banner Detection
Summary This script tries to detect the banner of an IRC server.
Vulnerability Detection Result The IRC server banner is: :irc.Metasploitable.LAN 351 CCGDAAJAE Unreal3.2.8.1. irc.Metasploitable.LAN :Fhi ↪X0oE [*=2309]
Log Method Details: IRC Server Banner Detection OID:1.3.6.1.4.1.25623.1.0.11156 Version used: \$Revision: 13541 \$

Log (CVSS: 0.0) NVT: Service Detection with 'GET' Request
Summary This plugin performs service detection. This plugin is a complement of find_service.nasl. It sends a 'GET' request to the remaining unknown services and tries to identify them.
Vulnerability Detection Result An IRC server seems to be running on this port.
Log Method Details: Service Detection with 'GET' Request OID:1.3.6.1.4.1.25623.1.0.17975 Version used: \$Revision: 14067 \$

Log (CVSS: 0.0) NVT: UnrealIRCd Detection
Summary Detection of UnrealIRCd Daemon. This script sends a request to the server and gets the version from the response.
Vulnerability Detection Result Detected UnrealIRCd Version: 3.2.8.1 Location: 6667/tcp CPE: cpe:/a:unrealircd:unrealircd:3.2.8.1 Concluded from version/product identification result: Unreal3.2.8.1
... continues on next page ...

...continued from previous page ...

Log Method

Details: UnrealIRCd Detection

OID:1.3.6.1.4.1.25623.1.0.809884

Version used: \$Revision: 10987 \$

[\[return to 10.0.2.4 \]](#)

Log 445/tcp

Log (CVSS: 0.0)

NVT: Microsoft SMB Signing Disabled

Summary

Checking for SMB signing is disabled.

The script logs in via smb, checks the SMB Negotiate Protocol response to confirm SMB signing is disabled.

Vulnerability Detection Result

SMB signing is disabled on this host

Log Method

Details: Microsoft SMB Signing Disabled

OID:1.3.6.1.4.1.25623.1.0.802726

Version used: \$Revision: 11003 \$

Log (CVSS: 0.0)

NVT: Microsoft Windows SMB Accessible Shares

Summary

The script detects the Windows SMB Accessible Shares and sets the result into KB.

Vulnerability Detection Result

The following shares were found

IPC\$

Log Method

Details: Microsoft Windows SMB Accessible Shares

OID:1.3.6.1.4.1.25623.1.0.902425

Version used: \$Revision: 11420 \$

Log (CVSS: 0.0)

NVT: SMB log in

... continues on next page ...

...continued from previous page ...
Summary This script attempts to logon into the remote host using login/password credentials.
Vulnerability Detection Result It was possible to log into the remote host using the SMB protocol.
Log Method Details: SMB log in OID:1.3.6.1.4.1.25623.1.0.10394 Version used: \$Revision: 13247 \$

Log (CVSS: 0.0) NVT: SMB Login Successful For Authenticated Checks
Summary It was possible to login using the provided SMB credentials. Hence authenticated checks are enabled.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Log Method Details: SMB Login Successful For Authenticated Checks OID:1.3.6.1.4.1.25623.1.0.108539 Version used: \$Revision: 13248 \$

Log (CVSS: 0.0) NVT: SMB NativeLanMan
Summary It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.
Vulnerability Detection Result Detected Samba Version: 3.0.20 Location: 445/tcp CPE: cpe:/a:samba:samba:3.0.20 Concluded from version/product identification result: Samba 3.0.20-Debian Extra information: Detected SMB workgroup: WORKGROUP Detected SMB server: Samba 3.0.20-Debian
Log Method ... continues on next page ...

...continued from previous page ...

Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: \$Revision: 13813 \$

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary

It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result

Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.0.20-Debian
Detected OS: Debian GNU/Linux

Log Method

Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: \$Revision: 13813 \$

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary

Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Vulnerability Detection Result

Only SMBv1 is enabled on remote target

Log Method

Details: SMB Remote Version Detection
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: \$Revision: 10898 \$

Log (CVSS: 0.0)
NVT: SMB Test with 'smbclient'

Summary

This script reports information about the SMB server of the remote host collected with the 'smbclient' tool.

Vulnerability Detection Result

... continues on next page ...

...continued from previous page ...
OS Version = UNIX Domain = WORKGROUP SMB Serverversion = SAMBA 3.0.20-DEBIAN
Log Method Details: SMB Test with 'smbclient' OID:1.3.6.1.4.1.25623.1.0.90011 Version used: \$Revision: 13274 \$

Log (CVSS: 0.0) NVT: SMB/CIFS Server Detection
Summary This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.
Vulnerability Detection Result A CIFS server is running on this port
Log Method Details: SMB/CIFS Server Detection OID:1.3.6.1.4.1.25623.1.0.11011 Version used: \$Revision: 13541 \$

[\[return to 10.0.2.4 \]](#)

Log 5900/tcp

Log (CVSS: 0.0) NVT: VNC security types
Summary This script checks the remote VNC protocol version and the available 'security types'.
Vulnerability Detection Result The remote VNC server chose security type #2 (VNC authentication)
Log Method Details: VNC security types OID:1.3.6.1.4.1.25623.1.0.19288 Version used: \$Revision: 13541 \$

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 003.003
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: 13541 \$

[\[return to 10.0.2.4 \]](#)

This file was automatically generated.