Scan Report

December 9, 2016

Summary

This document reports on the results of an automatic security scan. The scan started at Fri Dec 9 06:59:12 2016 UTC and ended at Fri Dec 9 07:14:11 2016 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

Host	High	Medium	Low	Log	False Positive
10.0.1.101	51	83	15	68	0
Total: 1	51	83	15	68	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 217 results selected by the filtering described above. Before filtering there were 217 results.

2 Results per Host

2.1 10.0.1.101

Host scan start Fri Dec 9 06:59:54 2016 UTC
Host scan end Fri Dec 9 07:13:58 2016 UTC

Service (Port)	Threat Level
general/tcp	High
8787/tcp	High
80/tcp	High
6000/tcp	High
445/tcp	High
2121/tcp	High
21/tcp	High
1524/tcp	High
3632/tcp	High
3306/tcp	High
5432/tcp	High
22/tcp	High
53/udp	High
53/tcp	High
6200/tcp	High
general/tcp	Medium
80/tcp	Medium
445/tcp	Medium
2121/tcp	Medium
21/tcp	Medium

... (continues) ...

... (continued) ...

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

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Summary
`OS End Of Life Detection`

... continues on next page ...

... continued from previous page ...

The Operating System on the remote host has reached the end of life and should not be used anymore

OID of test routine: 1.3.6.1.4.1.25623.1.0.103674

Vulnerability Detection Result

```
The Operating System (cpe:/o:canonical:ubuntu_linux:9.04) on the remote host has
↪ reached the end of life at 23 Oct 2010
and should not be used anymore.
See https://wiki.ubuntu.com/Releases for more information.
```

Vulnerability Detection Method

Details:OS End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: $Revision: 4111 $

[return to 10.0.1.101]

2.1.2 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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.108010

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:1562:in `syscall'\"0/usr/li
↪b/ruby/1.8/drb/drb.rb:1562:in `send'\"4/usr/lib/ruby/1.8/drb/drb.rb:1562:in `_
↪_send__'\"A/usr/lib/ruby/1.8/drb/drb.rb:1562:in `perform_without_block'\"3/usr
↪/lib/ruby/1.8/drb/drb.rb:1522:in `perform'\"5/usr/lib/ruby/1.8/drb/drb.rb:1596
↪:in `main_loop'\"0/usr/lib/ruby/1.8/drb/drb.rb:1592:in `loop'\"5/usr/lib/ruby/
```

... continues on next page ...

... continued from previous page ...

```
↪1.8/drb/drb.rb:1592:in `main_loop'\"1/usr/lib/ruby/1.8/drb/drb.rb:1588:in `sta
↪rt'\"5/usr/lib/ruby/1.8/drb/drb.rb:1588:in `main_loop'\"//usr/lib/ruby/1.8/drb
↪/drb.rb:1437:in `run'\"1/usr/lib/ruby/1.8/drb/drb.rb:1434:in `start'\"//usr/li
↪b/ruby/1.8/drb/drb.rb:1434:in `run'\"6/usr/lib/ruby/1.8/drb/drb.rb:1354:in `in
↪itialize'\"//usr/lib/ruby/1.8/drb/drb.rb:1634:in `new'\"9/usr/lib/ruby/1.8/drb
↪/drb.rb:1634:in `start_service'\"%/usr/sbin/druby_timeserver.rb:12:mesg\"Funct
↪ion not implemented:errnoi+
```

Impact

```
By default, Distributed Ruby does not impose restrictions on allowed hosts or se
↪t 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 exec
↪ute 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

```
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 ar
↪e allowed to submit Ruby commands, and >=3 may be appropriate)
  - 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: 4387 $`

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_t
↪esters/
   URL:http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html
```

[return to 10.0.1.101]

2.1.3 High 80/tcp

High (CVSS: 10.0)
NVT: PHP 'type confusion' Denial of Service Vulnerability (Linux)

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.808673

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.
  Impact Level: Application
```

Solution

```
Upgrade to PHP version 5.6.7
  or later. For updates refer to http://www.php.net
```

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' script
↪s.
```

Vulnerability Detection Method

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

Details:PHP 'type confusion' Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.808673
Version used: $Revision: 4497 $

References

```
CVE: CVE-2015-4601
BID:75246
Other:
```

...continues on next page ...

... continued from previous page ...

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

High (CVSS: 10.0)
NVT: PHP Heap-based buffer overflow in 'mbstring' extension

Summary

The host is running PHP and is prone to Buffer Overflow vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.900185

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.
Impact Level: Application

Solution

Upgrade to version 5.2.7 or later,
http://www.php.net/downloads.php

Vulnerability Insight

The flaw is due to error in mbfilter_htmlent.c file in the mbstring extension. These can be exploited via mb_convert_encoding, mb_check_encoding, mb_convert_variables, and mb_parse_str functions.

Vulnerability Detection Method

Details:PHP Heap-based buffer overflow in 'mbstring' extension
OID:1.3.6.1.4.1.25623.1.0.900185
Version used: $Revision: 4505 $

References

CVE: CVE-2008-5557
BID:32948
Other:
URL:http://bugs.php.net/bug.php?id=45722

... continues on next page ...

... continued from previous page ...

URL:http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0477.html

High (CVSS: 9.3)
NVT: PHP '_gdGetColors()' Buffer Overflow Vulnerability

Summary

The host is running PHP and is prone to Buffer Overflow
vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.801123

Vulnerability Detection Result

Installed version: 5.2.4
Fixed version: 5.2.11/5.3.1

Impact

Successful exploitation could allow attackers to potentially compromise a
vulnerable system.
Impact Level: System

Solution

Apply patches from SVN repository,
http://svn.php.net/viewvc?view=revision&revision=289557
*****
NOTE: Ignore this warning if patch is already applied.
*****

Vulnerability Insight

The flaw is due to error in '_gdGetColors' function in gd_gd.c which fails to
check certain colorsTotal structure member, whicn 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: 4504 $

References

CVE: CVE-2009-3546

... continues on next page ...

... continued from previous page ...

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: phpinfo() output accessible

Summary

Many PHP installation tutorials instruct the user to create
a file called phpinfo.php or similar containing the phpinfo() statement. Such
↪a file is often times
left in webserver directory after completion.

OID of test routine: 1.3.6.1.4.1.25623.1.0.11229

Vulnerability Detection Result

The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information to the remote attacker:
http://10.0.1.101/phpinfo.php
http://10.0.1.101/mutillidae/phpinfo.php

Impact

Some of the information that can be gathered from this file includes:
The username of the user who installed php, if they are a SUDO user, the IP ad
↪dress of the host, the web server
version, the system version(unix / linux), and the root directory of the web s
↪erver.

Solution

Delete them or restrict access to the listened files.

Vulnerability Detection Method

Details:phpinfo() output accessible
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: $Revision: 3669 $

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.900842

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

Impact
Successful exploitation could allow remote attackers to bypass intended access restrictions in the context of the affected application, and can cause the arbitrary command injection.
Impact Level: Application

Solution
Upgrade to Apache HTTP Server version 2.2.15 or later
For updates refer to http://www.apache.org/

Vulnerability Insight
The flaw is due to error in the mod_proxy_ftp module which can be exploited via vectors related to the embedding of these commands in the Authorization HTTP header.

Vulnerability Detection Method
Details:Apache 'mod_proxy_ftp' Module Command Injection Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.900842
Version used: $Revision: 3386 $

References
CVE: CVE-2009-3095
BID:36254
Other:
URL:http://intevydis.com/vd-list.shtml
URL:http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

High (CVSS: 7.1)
NVT: Apache 'mod_proxy_http.c' Denial Of Service Vulnerability

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.800827

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

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

Solution
Fixed in the SVN repository.
http://svn.apache.org/viewvc?view=rev&revision=790587

Vulnerability Insight
The flaw is due to error in 'stream_reqbody_cl' function in 'mod_proxy_http.c' in the mod_proxy module. When a reverse proxy is configured, it does not properly handle an amount of streamed data that exceeds the Content-Length value via crafted requests.

Vulnerability Detection Method
Details:Apache 'mod_proxy_http.c' Denial Of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800827
Version used: $Revision: 3386 $

References
CVE: CVE-2009-1890
BID:35565
Other:
URL:http://secunia.com/advisories/35691
URL:http://www.vupen.com/english/advisories/2009/1773
URL:http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=79058

... continues on next page ...

... continued from previous page ...

↪6&pathrev=790587

High (CVSS: 7.1)
NVT: Apache 'mod_deflate' Denial Of Service Vulnerability - July09

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.800837

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

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

Solution

Fixed in the SVN repository.
http://svn.apache.org/viewvc?view=rev&revision=791454
******
NOTE: Ignore this warning if above mentioned patch is already applied.
******

Vulnerability Insight

The flaw is due to error in 'mod_deflate' module which can cause a high CPU load by requesting large files which are compressed and then disconnecting.

Vulnerability Detection Method

Details:Apache 'mod_deflate' Denial Of Service Vulnerability - July09
OID:1.3.6.1.4.1.25623.1.0.800837
Version used: $Revision: 3386 $

References

CVE: CVE-2009-1891
BID:35623
Other:

... continues on next page ...

... continued from previous page ...

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: 7.1)
NVT: PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.808613

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 corrupt
↪ion)
by leveraging an application that performs many temporary-file accesses.
Impact Level: Application

Solution
Upgrade to PHP version 5.5.28, or 5.6.12,
or later. For updates refer to http://www.php.net

Vulnerability Insight
The flaw is due to script
'main/php_open_temporary_file.c' does not ensure thread safety.

Vulnerability Detection Method
Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.808613
Version used: $Revision: 4497 $

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2015-8878
BID:90837
Other:
URL:http://www.php.net/ChangeLog-5.php

[return to 10.0.1.101]

2.1.4 High 6000/tcp

High (CVSS: 10.0)
NVT: X Server

Summary
This plugin detects X Window servers.
X11 is a client - server protocol. Basically, the server is in charge of the screen, and the clients connect to it and send several requests like drawing a window or a menu, and the server sends events back to the clients, such as mouse clicks, key strokes, and so on...
An improperly configured X server will accept connections from clients from anywhere. This allows an attacker to make a client connect to the X server to record the keystrokes of the user, which may contain sensitive information, such as account passwords.
This can be prevented by using xauth, MIT cookies, or preventing the X server from listening on TCP (a Unix sock is used for local connections)

OID of test routine: 1.3.6.1.4.1.25623.1.0.10407

Vulnerability Detection Result
This X server does *not* allow any client to connect to it
however it is recommended that you filter incoming connections
to this port as attacker may send garbage data and slow down
your X session or even kill the server.
Here is the server version : 11.0
Here is the message we received : Client is not authorized
Solution: filter incoming connections to ports 6000-6009

Vulnerability Detection Method
Details:X Server

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.10407
Version used: $Revision: 2837 $

References
CVE: CVE-1999-0526

[return to 10.0.1.101]

2.1.5 High 445/tcp

High (CVSS: 10.0)
NVT: Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability

Summary
Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability

OID of test routine: 1.3.6.1.4.1.25623.1.0.105231

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

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
Updates are available. Please see the references or vendor advisory for more inf
↪ormation.

Vulnerability Insight
The Netlogon server implementation in smbd performs a free operation on an
uninitialized stack pointer, which allows remote attackers to execute arbitrar
↪y code via crafted Netlogon packets
that use the ServerPasswordSet RPC API, as demonstrated by packets reaching th
↪e _netr_ServerPasswordSet function
in rpc_server/netlogon/srv_netlog_nt.c.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Check the version
Details:Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105231
Version used: $Revision: 4398 $

References
CVE: CVE-2015-0240
BID:72711
Other:
URL:http://www.securityfocus.com/bid/72711
URL:http://www.samba.org

High (CVSS: 7.5)
NVT: Samba 'mount.cifs' Utility Symlink Attack Local Privilege Escalation Vulnerability

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100623

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.0.38/3.3.13/3.4.8

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

Solution
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
Version used: $Revision: 4396 $

... continues on next page ...

... continued from previous page ...

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 'SMB1 Packet Chaining' Unspecified Remote Memory Corruption Vulnerability

Summary
Samba is prone to an unspecified memory-corruption vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100680

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.3.13

Impact
Attackers can exploit this issue to execute arbitrary code in the
context of the application. Failed attacks may cause a denial-of-service condi
↪tion.

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

Vulnerability Detection Method
Details:Samba 'SMB1 Packet Chaining' Unspecified Remote Memory Corruption Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100680
Version used: $Revision: 4396 $

References
CVE: CVE-2010-2063
BID:40884
Other:
URL:https://www.securityfocus.com/bid/40884
URL:http://www.samba.org

... continues on next page ...

... continued from previous page ...

URL:http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=873
URL:http://www.samba.org/samba/security/CVE-2010-2063.html

High (CVSS: 7.5)
NVT: Samba SID Parsing Remote Buffer Overflow Vulnerability

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100803

Vulnerability Detection Result

Installed version: 3.0.20
Fixed version: 3.5.5

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

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

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: 4396 $

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

High (CVSS: 7.5)
NVT: Samba 'mtab' Lock File Handling Local Denial of Service Vulnerability

Summary

Samba is prone to a local denial-of-service vulnerability that affects
the mounting utilities 'mount.cifs' and 'umount.cifs'.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103283

Vulnerability Detection Result

Installed version: 3.0.20
Fixed version: 3.6.1

Impact

A local attacker can exploit this issue to cause the mounting
utilities to abort, resulting in a denial-of-service condition.

Solution

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: 4398 $

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/

[return to 10.0.1.101]

2.1.6 High 2121/tcp

High (CVSS: 10.0)
NVT: ProFTPD Multiple Remote Vulnerabilities

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.801639

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

Impact
Successful exploitation may allow execution of arbitrary code or cause a
denial-of-service.
Impact Level: Application

Solution
Upgrade to ProFTPD version 1.3.3c or later,
For updates refer to http://www.proftpd.org/

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: 3356 $

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

... continues on next page ...

... continued from previous page ...

URL:http://bugs.proftpd.org/show_bug.cgi?id=3521
URL:http://www.zerodayinitiative.com/advisories/ZDI-10-229/

High (CVSS: 9.0)
NVT: ProFTPD Prior To 1.3.3g Use-After-Free Remote Code Execution Vulnerability

Summary

ProFTPD is prone to a remote code-execution vulnerability.
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.
ProFTPD prior to 1.3.3g are vulnerable.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103331

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

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

Vulnerability Detection Method

Details:ProFTPD Prior To 1.3.3g Use-After-Free Remote Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103331
Version used: $Revision: 3386 $

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

Summary

... continues on next page ...

... continued from previous page ...

This host is running ProFTPD Server and is prone to remote
SQL Injection vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.900507

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

Impact
Successful exploitation will allow remote attackers to execute arbitrary
SQL commands, thus gaining access to random user accounts.

Solution
Upgrade to the latest version 1.3.2rc3,
http://www.proftpd.org/

Vulnerability Insight
This flaw occurs because the server performs improper input sanitising,
- 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 substition 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: 3265 $

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 10.0.1.101]

2.1.7 High 21/tcp

High (CVSS: 10.0)
NVT: ProFTPD Multiple Remote Vulnerabilities

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.801639

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

Impact
Successful exploitation may allow execution of arbitrary code or cause a
denial-of-service.
Impact Level: Application

Solution
Upgrade to ProFTPD version 1.3.3c or later,
For updates refer to http://www.proftpd.org/

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: 3356 $

References
CVE: CVE-2010-3867, CVE-2010-4221
BID:44562
Other:

...continues on next page ...

... continued from previous page ...

URL:http://secunia.com/advisories/42052
URL:http://bugs.proftpd.org/show_bug.cgi?id=3519
URL:http://bugs.proftpd.org/show_bug.cgi?id=3521
URL:http://www.zerodayinitiative.com/advisories/ZDI-10-229/

High (CVSS: 9.0)
NVT: ProFTPD Prior To 1.3.3g Use-After-Free Remote Code Execution Vulnerability

Summary
ProFTPD is prone to a remote code-execution vulnerability.
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.
ProFTPD prior to 1.3.3g are vulnerable.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103331

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

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

Vulnerability Detection Method
Details:ProFTPD Prior To 1.3.3g Use-After-Free Remote Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103331
Version used: $Revision: 3386 $

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/

... continues on next page ...

. . . continued from previous page . . .

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103185

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 app
↪lication.

Solution
The repaired package can be downloaded from
 https://security.appspot.com/vsftpd.html. Please validate the package with its
↪signature.

Vulnerability Detection Method
Details:vsftpd Compromised Source Packages Backdoor Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: $Revision: 2521 $

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
   URL:http://vsftpd.beasts.org/

High (CVSS: 7.5)
NVT: ProFTPD Server SQL Injection Vulnerability

. . . continues on next page . . .

... continued from previous page ...

Summary

This host is running ProFTPD Server and is prone to remote SQL Injection vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.900507

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to execute arbitrary SQL commands, thus gaining access to random user accounts.

Solution

Upgrade to the latest version 1.3.2rc3, http://www.proftpd.org/

Vulnerability Insight

This flaw occurs because the server performs improper input sanitising,

- 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 substition 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: 3265 $

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 10.0.1.101]

2.1.8 High 1524/tcp

High (CVSS: 10.0)
NVT: Possible Backdoor: Ingreslock

Summary
A backdoor is installed on the remote host
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103549

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

Vulnerability Detection Method
Details:Possible Backdoor: Ingreslock
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: $Revision: 3062 $

[return to 10.0.1.101]

2.1.9 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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103553

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

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

Vulnerability Detection Method

Details:distcc Remote Code Execution Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103553
Version used: $Revision: 3565 $

References

```
CVE: CVE-2004-2687
Other:
  URL:http://distcc.samba.org/security.html
   URL:http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2687
   URL:http://archives.neohapsis.com/archives/bugtraq/2005-03/0183.html
```

[return to 10.0.1.101]

2.1.10 High 3306/tcp

High (CVSS: 9.3)
NVT: MySQL 5.x Unspecified Buffer Overflow Vulnerability

Summary

```
MySQL is prone to a buffer-overflow vulnerability because if fails to
perform adequate boundary checks on user-supplied data.
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.
This issue affects MySQL 5.x
 other versions may also be vulnerable.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100271

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

. . . continued from previous page . . .

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: 3911 $

References
BID:36242
Other:
URL:http://www.securityfocus.com/bid/36242
URL:http://www.mysql.com/
URL:http://intevydis.com/company.shtml

High (CVSS: 9.0)
NVT: MySQL weak password

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103551

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

Solution
Change the password as soon as possible.

Vulnerability Detection Method
Details:MySQL weak password
OID:1.3.6.1.4.1.25623.1.0.103551
Version used: $Revision: 3911 $

High (CVSS: 8.5)
NVT: MySQL 'sql_parse.cc' Multiple Format String Vulnerabilities

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

. . . continues on next page . . .

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.800842

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.
  Impact Level: Application
```

Solution
```
Upgrade to MySQL version 5.1.36 or later
  http://dev.mysql.com/downloads
```

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.
```

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: 3575 $

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: 7.5)
NVT: MySQL 5.0.51a Unspecified Remote Code Execution Vulnerability

Summary
```
MySQL 5.0.51a is prone to an unspecified remote code-execution
vulnerability.
Very few technical details are currently available.
```

... continues on next page ...

... continued from previous page ...

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.
This issue affects MySQL 5.0.51a
 other versions may also be
vulnerable.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100436

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

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: 3911 $

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

High (CVSS: 7.5)
NVT: MySQL Server Buffer Overflow Vulnerability (Linux)

Summary
The host is running MySQL and is prone to Buffer overflow
  Vulnerability

OID of test routine: 1.3.6.1.4.1.25623.1.0.901093

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

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation could allow attackers to execute
arbitrary code.
Impact Level: Application

Solution
Upgrade to MySQL Version 5.0.90 or 5.1.43 or 5.5.1 or later,
For updates refer to http://dev.mysql.com/downloads

Vulnerability Insight
The flaw is due to an error in application that allows remote
attackers to execute arbitrary code via unspecified vectors

Vulnerability Detection Method
Details:MySQL Server Buffer Overflow Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.901093
Version used: $Revision: 3386 $

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

[return to 10.0.1.101]

2.1.11 High 5432/tcp

High (CVSS: 9.0)
NVT: PostgreSQL weak password

Summary
It was possible to login into the remote PostgreSQL as user postgres using weak
↪credentials.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103552

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
It was possible to login as user postgres with password \"postgres\".

Solution
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: 3911 $

High (CVSS: 9.0)
NVT: PostgreSQL Multiple Vulnerabilities - Mar15 (Linux)

Summary
This host is running PostgreSQL and is
prone to multiple vulnerabilities.

OID of test routine: 1.3.6.1.4.1.25623.1.0.807518

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.
Impact Level: Application

Solution
Upgrade to version 9.1.20 or 9.2.15 or
9.3.11 or 9.4.6 or 9.5.1 or higher,
For updates refer to http://www.postgresql.org/download

Vulnerability Insight
Multiple flaws are due to the PostgreSQL
incorrectly handle certain regular expressions and certain configuration

... continues on next page ...

... continued from previous page ...

settings (GUCS) for users of PL/Java.

Vulnerability Detection Method
Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:PostgreSQL Multiple Vulnerabilities - Mar15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.807518
Version used: $Revision: 4261 $

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

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

Summary
PostgreSQL is prone to multiple security vulnerabilities.
Attackers can exploit these issues to bypass certain security
restrictions and execute arbitrary Perl or Tcl code.
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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100645

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

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

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Method
Details:PostgreSQL Multiple Security Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100645
Version used: $Revision: 3911 $

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

[return to 10.0.1.101]

2.1.12 High 22/tcp

High (CVSS: 9.0)
NVT: SSH Brute Force Logins with default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.
As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1
↪.25623.1.0.108013) might run into a
timeout the actual reporting of this vulnerability takes place in this NVT ins
↪tead. The script preference 'Report timeout'
allows you to configure if such an timeout is reported.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103239

Vulnerability Detection Result
It was possible to login with the following credentials <User>:<Password>
msfadmin:msfadmin
user:user

Solution
Change the password as soon as possible.

. . . continues on next page . . .

. . . continued from previous page . . .

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: 4508 $

High (CVSS: 8.5)
NVT: OpenSSH Multiple Vulnerabilities

Summary
This host is running OpenSSH and is prone
to multiple vulnerabilities.

OID of test routine: 1.3.6.1.4.1.25623.1.0.806052

Vulnerability Detection Result
Installed version: 5.1p1
Fixed version: 7.0

Impact
Successful exploitation will allow an attacker
to gain privileges, to conduct impersonation attacks, to conduct brute-force
attacks or cause a denial of service.
Impact Level: Application

Solution
Upgrade to OpenSSH 7.0 or later.
For updates refer to http://www.openssh.com

Vulnerability Insight
Multiple flaws are due to:
- Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in
monitor.c in sshd.
- Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd.
- vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request.

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

. . . continues on next page . . .

... continued from previous page ...

Details:OpenSSH Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.806052
Version used: $Revision: 4336 $

References
CVE: CVE-2015-6564, CVE-2015-6563, CVE-2015-5600
Other:
URL:http://seclists.org/fulldisclosure/2015/Aug/54
URL:http://openwall.com/lists/oss-security/2015/07/23/4

High (CVSS: 7.8)
NVT: OpenSSH 'auth_password' Denial of Service Vulnerability (Linux)

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.809154

Vulnerability Detection Result
Installed version: 5.1p1
Fixed version: 7.3

Impact
Successfully exploiting this issue allows
remote attackers to cause a denial of service (crypt CPU consumption).
Impact Level: Application

Solution
Upgrade to OpenSSH version 7.3 or later.
For updates refer to http://www.openssh.com

Vulnerability Insight
The flaw exists due to the auth_password
function in 'auth-passwd.c' script does not limit password lengths for
password authentication.

Vulnerability Detection Method
Get the installed version with the help

... continues on next page ...

... continued from previous page ...

of detect NVT and check the version is vulnerable or not.
Details:OpenSSH 'auth_password' Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.809154
Version used: $Revision: 4336 $

References
CVE: CVE-2016-6515
BID:92212
Other:
URL:http://www.openssh.com/txt/release-7.3
URL:http://openwall.com/lists/oss-security/2016/08/01/2

High (CVSS: 7.5)
NVT: OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability

Summary
OpenSSH is prone to a remote memory-corruption vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105001

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

Impact
An attacker can exploit this issue to execute arbitrary code in context of the application. Failed exploits may result in denial-of-service conditions.

Solution
Updates are available.

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

... continues on next page ...

... continued from previous page ...

Check the version.
Details:OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105001
Version used: $Revision: 4336 $

References
CVE: CVE-2014-1692
BID:65230
Other:
URL:http://www.securityfocus.com/bid/65230
URL:http://www.openssh.com

High (CVSS: 7.2)
NVT: OpenSSH Privilege Escalation Vulnerability - May16

Summary
This host is installed with openssh and
is prone to privilege escalation vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.807574

Vulnerability Detection Result
Installed version: 5.1p1
Fixed version: 7.2p2-3

Impact
Successfully exploiting this issue will allow
local users to gain privileges.
Impact Level: Application

Solution
Upgrade to OpenSSH version 7.2p2-3 or later.
For updates refer to http://www.openssh.com

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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:OpenSSH Privilege Escalation Vulnerability - May16
OID:1.3.6.1.4.1.25623.1.0.807574
Version used: $Revision: 4336 $

References
CVE: CVE-2015-8325
Other:
URL:https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html
URL:https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4
↪e10a65c91810f88755

[return to 10.0.1.101]

2.1.13 High 53/udp

High (CVSS: 7.8)
NVT: ISC BIND Denial of Service Vulnerability

Summary
ISC BIND is prone to a denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.106291

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
Upgrade to 9.9.9-P3, 9.9.9-S5, 9.10.4-P3, 9.11.0rc3 or later.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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 the version.
Details:ISC BIND Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.106291
Version used: $Revision: 4429 $

References

CVE: CVE-2016-2776
Other:
URL:https://kb.isc.org/article/AA-01419

High (CVSS: 7.8)
NVT: ISC BIND Delegation Handling Denial of Service Vulnerability

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.806080

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.
Impact Level: Application

Solution

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).
For updates refer to https://www.isc.org

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The flaw is due to ISC BIND does not handle
delegation chaining properly.

Vulnerability Detection Method
Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:ISC BIND Delegation Handling Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.806080
Version used: $Revision: 4445 $

References
CVE: CVE-2014-8500
Other:
URL:https://kb.isc.org/article/AA-01216/0/

High (CVSS: 7.8)
NVT: ISC BIND Denial of Service Vulnerability - 06 - Jan16

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.807200

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.
Impact Level: Application

Solution
Upgrade to ISC BIND version 9.9.7-P2
or 9.10.2-P3 or later. For updates refer to https://www.isc.org

... continues on next page ...

... continued from previous page ...

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

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

Details:`ISC BIND Denial of Service Vulnerability - 06 - Jan16`
OID:`1.3.6.1.4.1.25623.1.0.807200`
Version used: `$Revision: 4426 $`

References

```
CVE: CVE-2015-5477
BID:76092
Other:
  URL:https://kb.isc.org/article/AA-01272
```

High (CVSS: 7.8)
NVT: ISC BIND 'buffer.c' Script Remote Denial of Service Vulnerability - Jan16

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.807202

Vulnerability Detection Result

```
Installed version: 9.4.2
Fixed version:     9.9.7-P3
```

Impact

```
Successful exploitation will allow remote attackers
  to cause denial of service.
  Impact Level: Application
```

Solution

```
Upgrade to ISC BIND version 9.9.7-P3
  or 9.10.2-P4 or later. For updates refer to https://www.isc.org
```

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

The flaw is due to an error in 'buffer.c'
script in ISC BIND.

Vulnerability Detection Method

Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
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: 4429 $

References

CVE: CVE-2015-5722
BID:76605
Other:
URL:https://kb.isc.org/article/AA-01287

High (CVSS: 7.8)
NVT: ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability - Jan16

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.807203

Vulnerability Detection Result

Installed version: 9.4.2
Fixed version: 9.7.7

Impact

Successful exploitation will allow attackers
to cause denial of service.
Impact Level: Application

Solution

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

... continues on next page ...

... continued from previous page ...

↪.
For updates refer to https://www.isc.org

Vulnerability Insight

The flaw exist due to an error in DNS
RDATA Handling in ISC BIND.

Vulnerability Detection Method

Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
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: 4429 $

References

CVE: CVE-2012-5166
BID:55852
Other:
URL:https://kb.isc.org/article/AA-00801

High (CVSS: 7.6)
NVT: ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100458

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

... continues on next page ...

... continued from previous page ...

Updates are available. Please see the references for details.

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: 4433 $

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

[return to 10.0.1.101]

2.1.14 High 53/tcp

High (CVSS: 7.8)
NVT: ISC BIND Denial of Service Vulnerability

Summary
ISC BIND is prone to a denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.106291

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
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 ...

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 the version.
```
Details:`ISC BIND Denial of Service Vulnerability`
OID:`1.3.6.1.4.1.25623.1.0.106291`
Version used: `$Revision: 4429 $`

References

```
CVE: CVE-2016-2776
Other:
  URL:https://kb.isc.org/article/AA-01419
```

High (CVSS: 7.8)
NVT: ISC BIND Delegation Handling Denial of Service Vulnerability

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.806080

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.
  Impact Level: Application
```

Solution

```
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).
  For updates refer to https://www.isc.org
```

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

```
The flaw is due to ISC BIND does not handle
  delegation chaining properly.
```

Vulnerability Detection Method

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

Details:`ISC BIND Delegation Handling Denial of Service Vulnerability`
OID:`1.3.6.1.4.1.25623.1.0.806080`
Version used: `$Revision: 4445 $`

References

```
CVE: CVE-2014-8500
Other:
  URL:https://kb.isc.org/article/AA-01216/0/
```

High (CVSS: 7.8)
NVT: ISC BIND Denial of Service Vulnerability - 06 - Jan16

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.807200

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.
  Impact Level: Application
```

Solution

```
Upgrade to ISC BIND version 9.9.7-P2
  or 9.10.2-P3 or later. For updates refer to https://www.isc.org
```

... continues on next page ...

. . . continued from previous page . . .

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
Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:ISC BIND Denial of Service Vulnerability - 06 - Jan16
OID:1.3.6.1.4.1.25623.1.0.807200
Version used: $Revision: 4426 $

References
CVE: CVE-2015-5477
BID:76092
Other:
URL:https://kb.isc.org/article/AA-01272

High (CVSS: 7.8)
NVT: ISC BIND 'buffer.c' Script Remote Denial of Service Vulnerability - Jan16

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.807202

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.9.7-P3

Impact
Successful exploitation will allow remote attackers
to cause denial of service.
Impact Level: Application

Solution
Upgrade to ISC BIND version 9.9.7-P3
or 9.10.2-P4 or later. For updates refer to https://www.isc.org

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Insight

The flaw is due to an error in 'buffer.c'
script in ISC BIND.

Vulnerability Detection Method

Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
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: 4429 $

References

CVE: CVE-2015-5722
BID:76605
Other:
URL:https://kb.isc.org/article/AA-01287

High (CVSS: 7.8)
NVT: ISC BIND DNS RDATA Handling Remote Denial of Service Vulnerability - Jan16

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.807203

Vulnerability Detection Result

Installed version: 9.4.2
Fixed version: 9.7.7

Impact

Successful exploitation will allow attackers
to cause denial of service.
Impact Level: Application

Solution

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

... continues on next page ...

... continued from previous page ...

↪.
For updates refer to https://www.isc.org

Vulnerability Insight

The flaw exist due to an error in DNS
RDATA Handling in ISC BIND.

Vulnerability Detection Method

Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
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: 4429 $

References

CVE: CVE-2012-5166
BID:55852
Other:
URL:https://kb.isc.org/article/AA-00801

High (CVSS: 7.6)
NVT: ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100458

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

... continues on next page ...

... continued from previous page ...

Updates are available. Please see the references for details.

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: 4433 $

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

[return to 10.0.1.101]

2.1.15 High 6200/tcp

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103185

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 app
↪lication.

Solution
The repaired package can be downloaded from
https://security.appspot.com/vsftpd.html. Please validate the package with its

... continues on next page ...

... continued from previous page ...

↪signature.

Vulnerability Detection Method
Details:vsftpd Compromised Source Packages Backdoor Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: $Revision: 2521 $

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
URL:http://vsftpd.beasts.org/

[return to 10.0.1.101]

2.1.16 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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.902815

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 inje
↪cting a TCP RST packet.

Solution
Please see the referenced advisories for more information on obtaining

... continues on next page ...

... continued from previous page ...

and applying fixes.

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 TC
↪P 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: 4048 $

References

CVE: CVE-2004-0230
BID:10183
Other:
URL:http://xforce.iss.net/xforce/xfdb/15886
URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006
URL:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx
URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx
URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html

[return to 10.0.1.101]

2.1.17 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: PHP Zend and GD Multiple Denial of Service Vulnerabilities

Summary

This host is running PHP and is prone to multiple denial of
service vulnerabilities.

OID of test routine: 1.3.6.1.4.1.25623.1.0.801586

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: 5.2.15/5.3.5

Impact
Successful exploitation could allow local attackers to crash the affected application, denying service to legitimate users.
Impact Level: Application/Network

Solution
Upgrade to PHP 5.3.5 or later
For updates refer to http://www.php.net/downloads.php

Vulnerability Insight
The flaws are due to:
- An use-after-free error in the 'Zend' engine, which allows remote attackers to cause a denial of service.
- A stack-based buffer overflow in the 'GD' extension, which allows attackers to cause a denial of service.

Vulnerability Detection Method
Details:PHP Zend and GD Multiple Denial of Service Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.801586
Version used: $Revision: 4502 $

References
CVE: CVE-2010-4697, CVE-2010-4698
Other:
URL:http://bugs.php.net/52879
URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 6.8)
NVT: PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)

Summary
This host is installed with PHP and is prone to multiple denial of service vulnerabilities.

OID of test routine: 1.3.6.1.4.1.25623.1.0.806649

. . . continues on next page . . .

... continued from previous page ...

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).
Impact Level: Application

Solution
Upgrade to PHP 5.5.30 or 5.6.14 or
later. For updates refer to http://www.php.net

Vulnerability Insight
Multiple flaws are due to,
- An Off-by-one error in the 'phar_parse_zipfile' function within ext/phar/zip
↪.c
script.
- An error in the 'phar_get_entry_data' function in ext/phar/util.c script.

Vulnerability Detection Method
Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.806649
Version used: $Revision: 4498 $

References
CVE: CVE-2015-7804, CVE-2015-7803
BID:76959
Other:
URL:http://www.php.net/ChangeLog-5.php
URL:https://bugs.php.net/bug.php?id=70433
URL:http://www.openwall.com/lists/oss-security/2015/10/05/8

Medium (CVSS: 6.4)
NVT: PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)

... continues on next page ...

... continued from previous page ...

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.809139

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.
Impact Level: Application

Solution

Upgrade to PHP version 5.5.31, or 5.6.17,
or 7.0.2, or later.
For updates refer to http://www.php.net

Vulnerability Insight

The flaw is due to the 'sapi/fpm/fpm/fpm_log.c'
script misinterprets the semantics of the snprintf return value.

Vulnerability Detection Method

Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)
OID:1.3.6.1.4.1.25623.1.0.809139
Version used: $Revision: 4497 $

References

CVE: CVE-2016-5114
BID:81808
Other:
URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 5.0)
NVT: PHP 'zend_strtod()' Function Floating-Point Value Denial of Service Vulnerability

Summary
PHP is prone to a remote denial-of-service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103020

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

Vulnerability Insight
The vulnerability is due to the Floating-Point Value that exist in zend_strtod f
↪unction

Vulnerability Detection Method
Details:PHP 'zend_strtod()' Function Floating-Point Value Denial of Service Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.103020
Version used: $Revision: 4502 $

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 Denial Of Service Vulnerability - April09

Summary

```
The host is installed with PHP and is prone to Denial of
  Service vulnerability.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.800393

Vulnerability Detection Result

```
Installed version: 5.2.4
Fixed version:     5.2.10
```

Impact

```
Successful exploitation could result in denial of service condition.
  Impact Level: Application
```

Solution

```
Upgrade to PHP version 5.2.9 or above,
  http://www.php.net/downloads.php
  Workaround:
  For workaround refer below link,
  http://cvs.php.net/viewvc.cgi/php-src/ext/json/JSON_parser.c?r1=1.1.2.14&r2=1.
↪1.2.15
```

Vulnerability Insight

```
Improper handling of .zip file while doing extraction via
  php_zip_make_relative_path function in php_zip.c file.
```

Vulnerability Detection Method

Details:PHP Denial Of Service Vulnerability - April09
OID:1.3.6.1.4.1.25623.1.0.800393
Version used: $Revision: 4504 $

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 'ext/imap/php_imap.c' Use After Free Denial of Service Vulnerability

Summary
This host is running PHP and is prone to denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.801583

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.
Impact Level: Application/Network

Solution
Upgrade to PHP 5.2.15 or 5.3.4
For updates refer to http://www.php.net/downloads.php

Vulnerability Insight
The flaw is due to an erron 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
OID:1.3.6.1.4.1.25623.1.0.801583
Version used: $Revision: 4502 $

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

Medium (CVSS: 5.0)
NVT: PHP Multiple Denial of Service Vulnerabilities (Linux)

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.808611

Vulnerability Detection Result

Installed version: 5.2.4
Fixed version: 5.6.12

Impact

Successfully exploiting this issue allow
remote attackers to cause a denial of service (application crash or
memory consuption).
Impact Level: Application

Solution

Upgrade to PHP version 5.6.12
or later. For updates refer to http://www.php.net

Vulnerability Insight

Multiple flaws are due to
- An improper handling of driver behavior for SQL_WVARCHAR columns in the
'odbc_bindcols function' in 'ext/odbc/php_odbc.c' script.
- The 'gdImageScaleTwoPass' function in gd_interpolation.c script in the
GD Graphics Library uses inconsistent allocate and free approaches.

Vulnerability Detection Method

Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:PHP Multiple Denial of Service Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.808611
Version used: $Revision: 4497 $

References

CVE: CVE-2015-8877, CVE-2015-8879, CVE-2015-8874
BID:90866, 90842, 90714

... continues on next page ...

... continued from previous page ...

Other:
URL:http://www.php.net/ChangeLog-5.php

Medium (CVSS: 5.0)
NVT: PHP 'unserialize()' Function Denial of Service Vulnerability

Summary
The host is running PHP and is prone to Denial of Service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.900993

Vulnerability Detection Result
Installed version: 5.2.4
Fixed version: N/A

Impact
Successful exploitation could allow attackers to execute arbitrary PHP code and cause denial of service.
Impact Level: Application

Solution
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Vulnerability Insight
An error in 'unserialize()' function while processing malformed user supplied data containing a long serialized string passed via the '__wakeup()' or '__destruct()' methods.

Vulnerability Detection Method
Details:PHP 'unserialize()' Function Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.900993
Version used: $Revision: 4505 $

References
CVE: CVE-2009-4418

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://www.security-database.com/detail.php?alert=CVE-2009-4418
   URL:http://www.suspekt.org/downloads/POC2009-ShockingNewsInPHPExploitation.pd
↪f
```

[return to 10.0.1.101]

2.1.18 Medium 445/tcp

Medium (CVSS: 6.8)
NVT: Samba 'mount.cifs' Utility Local Privilege Escalation Vulnerability

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100476

Vulnerability Detection Result

```
Installed version: 3.0.20
Fixed version:     3.4.6
```

Impact

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

Solution

```
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: 4396 $

References

```
CVE: CVE-2009-3297, CVE-2010-0787
BID:37992
Other:
  URL:http://www.securityfocus.com/bid/37992
```

... continues on next page ...

... continued from previous page ...

URL:http://www.samba.org

Medium (CVSS: 6.8)
NVT: Samba Badlock Critical Vulnerability

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.807646

Vulnerability Detection Result

Installed version: 3.0.20
Fixed version: 4.2.11 or 4.3.8 or 4.4.2, or later

Impact

Successful exploitation of this vulnerability
leads to Man-in-the-middle (MITM) attacks, to causes denial of service, to spo
↪of
and to obtain sensitive session information.
Impact Level: Application

Solution

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

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 connec
↪tions.
- 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 connection
↪s.
- An error in the implementation of NTLMSSP authentication.
-

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method

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

Details:Samba Badlock Critical Vulnerability
OID:1.3.6.1.4.1.25623.1.0.807646
Version used: $Revision: 4401 $

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
```

Medium (CVSS: 6.0)
NVT: Samba multiple vulnerabilities

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 vulnerabil
↪ity.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100306

Vulnerability Detection Result

```
Installed version: 3.0.20
Fixed version:     3.0.37/3.2.15/3.3.8/3.4.2
```

Impact

```
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

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:Samba multiple vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100306
Version used: $Revision: 4393 $

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: 6.0)
NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)

Summary
Samba is prone to a vulnerability that allows attackers to execute arbitrary she
↪ll
commands because the software fails to sanitize user-supplied input.

OID of test routine: 1.3.6.1.4.1.25623.1.0.108011

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

Impact
An attacker may leverage this issue to execute arbitrary shell commands on an af
↪fected
system with the privileges of the application.

Solution
Updates are available. Please see the referenced vendor advisory.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Send a crafted command to the samba server and check for a remote command execut
↪ion.
Details:Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)
OID:1.3.6.1.4.1.25623.1.0.108011
Version used: $Revision: 4401 $

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 MS-RPC Remote Shell Command Execution Vulnerability (Version Check)

Summary
Samba is prone to a vulnerability that allows attackers to execute arbitrary she
↪ll
commands because the software fails to sanitize user-supplied input.

OID of test routine: 1.3.6.1.4.1.25623.1.0.108012

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: See referenced vendor advisory

Impact
An attacker may leverage this issue to execute arbitrary shell commands on an af
↪fected
system with the privileges of the application.

Solution
Updates are available. Please see the referenced vendor advisory.

Vulnerability Detection Method
Get the installed version with the help of the Detection NVT and check if the ve

... continues on next page ...

... continued from previous page ...

↪rsion is vulnerable or not.
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: 4401 $

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: 5.0)
NVT: Samba 'FD_SET' Memory Corruption Vulnerability

Summary
Samba is prone to a memory-corruption vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103095

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.5.7

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
this has not been confirmed.

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

Vulnerability Detection Method
Details:Samba 'FD_SET' Memory Corruption Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103095
Version used: $Revision: 4398 $

References

... continues on next page ...

... continued from previous page ...

```
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: 5.0)
NVT: Samba winbind Daemon Denial of Service Vulnerability

Summary

```
This host is installed with Samba for Linux and is prone to
  Winbind daemon Denial of Service Vulnerability.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.800711

Vulnerability Detection Result

```
Installed version: 3.0.20
Fixed version:     3.0.32
```

Impact

```
Successful exploitation will let the attacker crash the application.
  Impact level: Application
```

Solution

```
Upgrade to the latest version 3.0.32
  http://us1.samba.org/samba
```

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: 4393 $`

References

... continues on next page ...

... continued from previous page ...

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 10.0.1.101]

2.1.19 Medium 2121/tcp

Medium (CVSS: 5.8)
NVT: ProFTPD mod_tls Module NULL Character CA SSL Certificate Validation Security Bypass Vulnerability

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.
Successful exploits allows attackers to perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks.
Versions prior to ProFTPD 1.3.2b and 1.3.3 to 1.3.3.rc1 are vulnerable.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100316

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

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:ProFTPD mod_tls Module NULL Character CA SSL Certificate Validation Security By.
↪..
OID:1.3.6.1.4.1.25623.1.0.100316
Version used: $Revision: 3263 $

References
CVE: CVE-2009-3639
BID:36804

... continues on next page ...

... continued from previous page ...

Other:
URL:http://www.securityfocus.com/bid/36804
URL:http://bugs.proftpd.org/show_bug.cgi?id=3275
URL:http://www.proftpd.org

Medium (CVSS: 4.0)
NVT: ProFTPD Denial of Service Vulnerability

Summary
The host is running ProFTPD and is prone to denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.801640

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

Impact
Successful exploitation will allow attackers to cause a denial of service.
Impact Level: Application

Solution
Upgrade to ProFTPD version 1.3.2rc3 or later,
For updates refer to http://www.proftpd.org/

Vulnerability Insight
The flaw is due to an error in 'pr_data_xfer()' function which allows remote authenticated users to cause a denial of service (CPU consumption) via an ABOR command during a data transfer.

Vulnerability Detection Method
Details:ProFTPD Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801640
Version used: $Revision: 3166 $

References
CVE: CVE-2008-7265
Other:
URL:http://bugs.proftpd.org/show_bug.cgi?id=3131

[return to 10.0.1.101]

2.1.20 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Check for Anonymous FTP Login

Summary
This FTP Server allows anonymous logins.

OID of test routine: 1.3.6.1.4.1.25623.1.0.900600

Vulnerability Detection Result
It was possible to login to the remote FTP service with the following anonymous account:
anonymous:openvas@example.com
ftp:openvas@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
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
Try to login with an anonymous account at the remove FTP service.
Details:Check for Anonymous FTP Login
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: $Revision: 4406 $

... continues on next page ...

... continued from previous page ...

References
Other:
URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497

Medium (CVSS: 5.8)
NVT: ProFTPD mod_tls Module NULL Character CA SSL Certificate Validation Security Bypass Vulnerability

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.
Successful exploits allows attackers to perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks.
Versions prior to ProFTPD 1.3.2b and 1.3.3 to 1.3.3.rc1 are vulnerable.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100316

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

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:ProFTPD mod_tls Module NULL Character CA SSL Certificate Validation Security By.
↪..
OID:1.3.6.1.4.1.25623.1.0.100316
Version used: $Revision: 3263 $

References
CVE: CVE-2009-3639
BID:36804
Other:
URL:http://www.securityfocus.com/bid/36804
URL:http://bugs.proftpd.org/show_bug.cgi?id=3275
URL:http://www.proftpd.org

Medium (CVSS: 5.1)
NVT: vsftpd '_tzfile_read()' Function Heap Based Buffer Overflow Vulnerability

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103362

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

Impact
Attackers may leverage this issue to execute arbitrary code in the
context of the application. Failed attacks will cause denial-of-service conditi
↪ons.

Vulnerability Detection Method
Details:vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103362
Version used: $Revision: 3386 $

References
BID:51013
Other:
URL:http://www.securityfocus.com/bid/51013
URL:http://dividead.wordpress.com/tag/heap-overflow/
URL:http://vsftpd.beasts.org/

Medium (CVSS: 4.0)
NVT: ProFTPD Denial of Service Vulnerability

Summary
The host is running ProFTPD and is prone to denial of service
vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.801640

... continues on next page ...

. . . continued from previous page . . .

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

Impact
Successful exploitation will allow attackers to cause a denial of service.
Impact Level: Application

Solution
Upgrade to ProFTPD version 1.3.2rc3 or later,
For updates refer to http://www.proftpd.org/

Vulnerability Insight
The flaw is due to an error in 'pr_data_xfer()' function which allows
remote authenticated users to cause a denial of service (CPU consumption)
via an ABOR command during a data transfer.

Vulnerability Detection Method
Details:ProFTPD Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801640
Version used: $Revision: 3166 $

References
CVE: CVE-2008-7265
Other:
URL:http://bugs.proftpd.org/show_bug.cgi?id=3131

[return to 10.0.1.101]

2.1.21 Medium 3306/tcp

Medium (CVSS: 6.8)
NVT: MySQL Denial Of Service and Spoofing Vulnerabilities

Summary
The host is running MySQL and is prone to Denial Of Service
and Spoofing Vulnerabilities

OID of test routine: 1.3.6.1.4.1.25623.1.0.801064

. . . continues on next page . . .

... continued from previous page ...

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

Impact
```
Successful exploitation could allow users to cause a Denial of Service and
  man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via
  a crafted certificate.
  Impact Level: Application
```

Solution
```
Upgrade to MySQL version 5.0.88 or 5.1.41
  For updates refer to http://dev.mysql.com/downloads
```

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: 3238 $`

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
```

Medium (CVSS: 6.5)
NVT: MySQL Multiple Vulnerabilities

Summary
```
The host is running MySQL and is prone to multiple vulnerabilities.
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.801355

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

Impact
```
Successful exploitation could allow users to cause a denial of service and
  to execute arbitrary code.
  Impact Level: Application
```

Solution
```
Upgrade to MySQL version 5.0.91 or 5.1.47,
  For updates refer to http://dev.mysql.com/downloads
```

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 remot
↪e
    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.
```

Vulnerability Detection Method
Details:MySQL Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.801355
Version used: $Revision: 3152 $

References
```
CVE: CVE-2010-1848, CVE-2010-1849, CVE-2010-1850
Other:
  URL:http://securitytracker.com/alerts/2010/May/1024031.html
   URL:http://securitytracker.com/alerts/2010/May/1024033.html
   URL:http://securitytracker.com/alerts/2010/May/1024032.html
   URL:http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html
   URL:http://dev.mysql.com/doc/refman/5.0/en/news-5-0-91.html
```

Medium (CVSS: 6.0)
NVT: MySQL Authenticated Access Restrictions Bypass Vulnerability (Linux)

Summary

```
The host is running MySQL and is prone to Access Restrictions Bypass
  Vulnerability
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.801065

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

```
Successful exploitation could allow users to bypass intended access restrictions
  by calling CREATE TABLE with  DATA DIRECTORY or INDEX DIRECTORY argument refer
↪ring
  to a subdirectory.
  Impact Level: Application
```

Solution

```
Upgrade to MySQL version 5.0.88 or 5.1.41 or 6.0.9-alpha
  For updates refer to http://dev.mysql.com/downloads
```

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: 3238 $`

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
```

Medium (CVSS: 5.0)
NVT: Oracle MySQL Prior to 5.1.51 Multiple Denial Of Service Vulnerabilities

Summary
MySQL is prone to multiple denial-of-service vulnerabilities.
An attacker can exploit these issues to crash the database, denying
access to legitimate users.
These issues affect versions prior to MySQL 5.1.51.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100900

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

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

Vulnerability Detection Method
Details: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: 3911 $

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: 5.0)
NVT: MySQL Multiple Denial of Service Vulnerabilities

Summary
The host is running MySQL and is prone to multiple denial of
service vulnerabilities.

OID of test routine: 1.3.6.1.4.1.25623.1.0.801571

. . . continues on next page . . .

... continued from previous page ...

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

Impact
```
Successful exploitation could allow an attacker to cause a denial of service
  and to execute arbitrary code.
  Impact Level: Application
```

Solution
```
Upgrade to MySQL version 5.0.92, or 5.1.51 or 5.5.6
  For updates refer to http://dev.mysql.com/downloads
```

Vulnerability Insight
```
The flaws are due to:
   - An error in propagating the type errors, which allows remote attackers
     to cause a denial of service via crafted arguments to extreme-value functio
↪ns
     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: 3386 $

References
```
CVE: CVE-2010-3833, CVE-2010-3834, CVE-2010-3836, CVE-2010-3837, CVE-2010-3838
BID:43676
Other:
  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
```

Medium (CVSS: 4.6)
NVT: MySQL MyISAM Table Privileges Secuity Bypass Vulnerability

Summary
```
According to its version number, the remote version of MySQL is
  prone to a security-bypass vulnerability.
  An attacker can exploit this issue to gain access to table files created by
  other users, bypassing certain security restrictions.
  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.
  This issue affects versions prior to MySQL 4 (prior to 4.1.24) and
  MySQL 5 (prior to 5.0.60).
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100156

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

Solution
```
Updates are available. Update to newer Version.
```

Vulnerability Detection Method
Details:`MySQL MyISAM Table Privileges Secuity Bypass Vulnerability`
OID:`1.3.6.1.4.1.25623.1.0.100156`
Version used: `$Revision: 3911 $`

References
```
CVE: CVE-2008-2079, CVE-2008-4097, CVE-2008-4098
BID:29106
Other:
  URL:http://www.securityfocus.com/bid/29106
```

Medium (CVSS: 4.4)
NVT: MySQL multiple Vulnerabilities

Summary
```
MySQL is prone to a security-bypass vulnerability and to to a local
privilege-escalation vulnerability.
An attacker can exploit the security-bypass issue to bypass certain
```
... continues on next page ...

... continued from previous page ...

security restrictions and obtain sensitive information that may lead
to further attacks.
Local attackers can exploit the local privilege-escalation issue to
gain elevated privileges on the affected computer.
Versions prior to MySQL 5.1.41 are vulnerable.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100356

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

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:MySQL multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100356
Version used: $Revision: 3911 $

References
CVE: CVE-2009-4030
BID:37075
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: 4.0)
NVT: Oracle MySQL 'TEMPORARY InnoDB' Tables Denial Of Service Vulnerability

Summary
MySQL is prone to a denial-of-service vulnerability.
An attacker can exploit these issues to crash the database, denying
access to legitimate users.
This issues affect versions prior to MySQL 5.1.49.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100763

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Detection Method
Details:Oracle MySQL 'TEMPORARY InnoDB' Tables Denial Of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100763
Version used: $Revision: 3911 $

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: 4.0)
NVT: Oracle MySQL Prior to 5.1.49 Multiple Denial Of Service Vulnerabilities

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100785

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

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

... continues on next page ...

... continued from previous page ...

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: 3911 $

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/

Medium (CVSS: 4.0)
NVT: MySQL Mysqld Multiple Denial Of Service Vulnerabilities

Summary
The host is running MySQL and is prone to multiple denial of service
vulnerabilities.

OID of test routine: 1.3.6.1.4.1.25623.1.0.801567

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.
Impact Level: Application

Solution
Upgrade to MySQL version 5.1.49 or 5.0.92

... continues on next page ...

... continued from previous page ...

For updates refer to http://dev.mysql.com/downloads

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.

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: 3386 $

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

Medium (CVSS: 4.0)
NVT: MySQL Empty Bit-String Literal Denial of Service Vulnerability

Summary

This host is running MySQL, which is prone to Denial of Service Vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.900221

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation by remote attackers could cause denying access to legitimate users.
Impact Level : Application

... continues on next page ...

... continued from previous page ...

Solution
Update to version 5.0.66 or 5.1.26 or 6.0.6 or later.
http://dev.mysql.com/downloads/

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: 4522 $

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

[return to 10.0.1.101]

2.1.22 Medium 5432/tcp

Medium (CVSS: 6.8)
NVT: PostgreSQL Multiple Security Vulnerabilities

Summary
PostgreSQL is prone to multiple security vulnerabilities, including a
denial-of-service issue, a privilege-escalation issue, and an authentication-
bypass issue.
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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100273

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Detection Method
Details:`PostgreSQL Multiple Security Vulnerabilities`
OID:`1.3.6.1.4.1.25623.1.0.100273`
Version used: `$Revision: 3911 $`

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#c1
   URL:http://www.postgresql.org/
   URL:http://www.postgresql.org/support/security
   URL:http://permalink.gmane.org/gmane.comp.security.oss.general/2088
```

Medium (CVSS: 6.8)
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)

Summary
`OpenSSL is prone to security-bypass vulnerability.`

OID of test routine: 1.3.6.1.4.1.25623.1.0.105043

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

... continues on next page ...

... continued from previous page ...

Updates are available.

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:OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)
OID:1.3.6.1.4.1.25623.1.0.105043
Version used: $Revision: 3967 $

References

CVE: CVE-2014-0224
BID:67899
Other:
URL:http://www.securityfocus.com/bid/67899
URL:http://openssl.org/

Medium (CVSS: 6.5)
NVT: PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability

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.
Successfully exploiting this issue allows attackers to perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks.
PostgreSQL is also prone to a local privilege-escalation vulnerability.
Exploiting this issue allows local attackers to gain elevated privileges.
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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100400

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Detection Method
Details:PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnera.
↪..
OID:1.3.6.1.4.1.25623.1.0.100400
Version used: $Revision: 3911 $

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: 6.5)
NVT: PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability

Summary
PostgreSQL is prone to a buffer-overflow vulnerability because the
application fails to perform adequate boundary checks on user-
supplied data.
Attackers can exploit this issue to execute arbitrary code with
elevated privileges or crash the affected application.
PostgreSQL version 8.0.x, 8.1.x, 8.3.x is vulnerable
other versions may also be affected.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100470

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100470
Version used: $Revision: 3911 $

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

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. 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. The issue affect versions prior to 8.2.20, 8.3.14, 8.4.7, and 9.0.3.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103054

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

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

Vulnerability Detection Method
Details:PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103054
Version used: $Revision: 3911 $

... continues on next page ...

. . . continued from previous page . . .

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: 6.5)
NVT: PostgreSQL Code Injection and Denial of Service Vulnerabilities (Linux)

Summary

```
This host is running PostgreSQL and is
  prone to code injection and denial of service vulnerabilities.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.808665

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.
  Impact Level: Application
```

Solution

```
Upgrade to version 9.1.23 or 9.2.18 or
  9.3.14 or 9.4.9 or 9.5.4 or higher,
  For updates refer to http://www.postgresql.org/download
```

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

```
Get the installed version with the help of
```

. . . continues on next page . . .

... continued from previous page ...

detect NVT and check the version is vulnerable or not.
Details:PostgreSQL Code Injection and Denial of Service Vulnerabilities (Linux)
OID:1.3.6.1.4.1.25623.1.0.808665
Version used: $Revision: 4161 $

References
CVE: CVE-2016-5423, CVE-2016-5424
BID:92433, 92435
Other:
URL:https://www.postgresql.org/about/news/1688/

Medium (CVSS: 6.0)
NVT: PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability

Summary
PostgreSQL is prone to a local privilege-escalation vulnerability.
Exploiting this issue allows local attackers to gain elevated
privileges and execute arbitrary commands with the privileges of
the victim.
Versions prior to PostgreSQL 9.0.1 are vulnerable.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100843

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

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

Vulnerability Detection Method
Details:PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100843
Version used: $Revision: 3911 $

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

... continues on next page ...

... continued from previous page ...

URL:http://www.postgresql.org
URL:http://www.postgresql.org/support/security

Medium (CVSS: 5.5)
NVT: PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability

Summary

PostgreSQL is prone to an unauthorized-access vulnerability.
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.
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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100648

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

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

Vulnerability Detection Method

Details:PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100648
Version used: $Revision: 3911 $

References

CVE: CVE-2010-1975
BID:40304
Other:
URL:http://www.securityfocus.com/bid/40304
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

... continues on next page ...

... continued from previous page ...

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: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103955

Vulnerability Detection Result
```
Expired Certificates:\
\
\
The certificate on 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: ED093088706603BFD5DC237399B498DA2D4D31C6\
\
The certificate on 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
```

... continues on next page ...

... continued from previous page ...

```
↪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: ED093088706603BFD5DC237399B498DA2D4D31C6
```

Solution

```
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 ex
↪pired.
```

Vulnerability Detection Method

Details:`SSL/TLS: Certificate Expired`
OID:`1.3.6.1.4.1.25623.1.0.103955`
Version used: `$Revision: 4614 $`

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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.111012

Vulnerability Detection Result

```
In addition to TLSv1+ the service is also providing the deprecated SSLv3 protoco
↪l and supports one or more ciphers. Those supported ciphers can be found in th
↪e 'Check SSL Weak Ciphers and Supported Ciphers' NVT.
```

Impact

```
An attacker might be able to use the known
  cryptographic flaws to eavesdrop the connection between clients and the servic
↪e
  to get access to sensitive data transferred within the secured connection.
```

... continues on next page ...

... continued from previous page ...

Solution

```
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.
```

Vulnerability Insight

```
The SSLv2 and SSLv3 protocols containing
  known cryptographic flaws.
```

Vulnerability Detection Method

```
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: 4616 $`

References

```
Other:
  URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/delivera
↪bles/algorithms-key-sizes-and-parameters-report
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

Medium (CVSS: 4.3)
NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

Summary

```
This host is prone to an information disclosure vulnerability.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802087

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.
  Impact Level: Application
```

... continues on next page ...

... continued from previous page ...

Solution
Disable SSL v3.0

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not cove
↪red by the Message Authentication Code

Vulnerability Detection Method
Send a SSLv3 request and check the response.
Details:POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: $Revision: 4161 $

References
CVE: CVE-2014-3566
BID:70574
Other:
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

Medium (CVSS: 4.3)
NVT: PostgreSQL Remote Denial Of Service Vulnerability June15 (Linux)

Summary
This host is running PostgreSQL and is
prone to remote denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.805805

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

Impact
Successful exploitation will allow a
remote attacker to crash the program.

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution

Upgrade to version 9.0.20, 9.1.16, 9.2.11,
9.3.7, 9.4.2 or higher, For updates refer to http://www.postgresql.org/downloa
↪d

Vulnerability Insight

Flaw is triggered when a timeout interrupt
is fired partway through the session shutdown sequence.

Vulnerability Detection Method

Get the installed version with the help of
detect NVT and check the version is vulnerable or not.
Details:PostgreSQL Remote Denial Of Service Vulnerability June15 (Linux)
OID:1.3.6.1.4.1.25623.1.0.805805
Version used: $Revision: 4161 $

References

CVE: CVE-2015-3165
BID:74787
Other:
URL:http://www.postgresql.org/about/news/1587

Medium (CVSS: 4.0)
NVT: PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability

Summary

PostgreSQL is prone to a remote denial-of-service vulnerability.
Exploiting this issue may allow attackers to terminate connections
to the PostgreSQL server, denying service to legitimate users.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100157

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Updates are available. Update to newer Version.

... continues on next page ...

... continued from previous page ...

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: 3911 $

References
CVE: CVE-2009-0922
BID:34090
Other:
URL:http://www.securityfocus.com/bid/34090
URL:http://www.postgresql.org/

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate chain that has been signed usi
↪ng a cryptographically weak hashing algorithm.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105880

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

Vulnerability Insight
Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not sec
↪ure enough for ongoing use. Beginning as late as January 2017
and as early as June 2016, browser developers such as Microsoft and Google wil
↪l begin warning users when users visit web sites that use SHA-1 signed Secure
↪Socket Layer (SSL)
certificates. Servers that use SSL/TLS certificates signed using an SHA-1 sign
↪ature will need to obtain new SHA-2 signed SSL/TLS certificates to avoid these
↪ web browser SSL/TLS certificate warnings.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Check which 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: 4614 $

References
Other:
URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

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).

OID of test routine: 1.3.6.1.4.1.25623.1.0.106223

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits\

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html)

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.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details:SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: $Revision: 4614 $

References
Other:
URL:https://weakdh.org/

[return to 10.0.1.101]

2.1.23 Medium 22/tcp

Medium (CVSS: 5.8)
NVT: OpenSSH 'child_set_env()' Function Security Bypass Vulnerability

Summary
OpenSSH is prone to a security-bypass vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105003

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

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

Solution
Updates are available.

Vulnerability Insight
sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Check the version.
Details:OpenSSH 'child_set_env()' Function Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105003
Version used: $Revision: 4336 $

References
CVE: CVE-2014-2532
BID:66355
Other:
URL:http://www.securityfocus.com/bid/66355
URL:http://www.openssh.com

Medium (CVSS: 5.8)
NVT: OpenSSH Certificate Validation Security Bypass Vulnerability

Summary
OpenSSH is prone to a security-bypass vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105004

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

Impact
Attackers can exploit this issue to bypass certain security
restrictions and perform unauthorized actions. This may aid in
further attacks.

Solution
Updates are available.

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

. . . continues on next page . . .

. . . continued from previous page . . .

Check the version
Details:OpenSSH Certificate Validation Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105004
Version used: $Revision: 4336 $

References
CVE: CVE-2014-2653
BID:66459
Other:
URL:http://www.securityfocus.com/bid/66459
URL:http://www.openssh.com

Medium (CVSS: 5.5)
NVT: OpenSSH ¡= 7.2p1 - Xauth Injection

Summary
openssh xauth command injection may lead to forced-command and /bin/false bypass

OID of test routine: 1.3.6.1.4.1.25623.1.0.105581

Vulnerability Detection Result
Installed version: 5.1p1
Fixed version: 7.2p2

Impact
By injecting xauth commands one gains limited* read/write arbitrary files, infor
↪mation leakage or xauth-connect capabilities.

Solution
Upgrade to OpenSSH version 7.2p2 or later.
For updates refer to http://www.openssh.com

Vulnerability Insight
An authenticated user may inject arbitrary xauth commands by sending an x11 chan
↪nel request that includes a newline character in the x11 cookie. The newline a
↪cts as a command separator to the xauth binary. This attack requires the serve
↪r to have 'X11Forwarding yes' enabled. Disabling it, mitigates this vector.

Vulnerability Detection Method

. . . continues on next page . . .

... continued from previous page ...

Get the installed version with the help of detect NVT and check the version is
↪vulnerable or not.
Details:OpenSSH <= 7.2p1 - Xauth Injection
OID:1.3.6.1.4.1.25623.1.0.105581
Version used: $Revision: 2970 $

References
CVE: CVE-2016-3115
Other:
URL:http://www.openssh.com/txt/release-7.2p2

Medium (CVSS: 5.0)
NVT: OpenSSH Denial of Service Vulnerability

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103939

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

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

Solution
Updates are available.

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

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 4336 $

References

```
CVE: CVE-2010-5107
BID:58162
Other:
  URL:http://www.securityfocus.com/bid/58162
   URL:http://www.openssh.com
```

Medium (CVSS: 5.0)
NVT: OpenSSH Denial of Service Vulnerability - Jan16

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.806671

Vulnerability Detection Result

```
Installed version: 5.1p1
Fixed version:     7.1p2
```

Impact

```
Successfully exploiting this issue allow
  remote attackers to cause a denial of service (out-of-bounds read and applicat
↪ion
  crash).
  Impact Level: Application
```

Solution

```
Upgrade to OpenSSH version 7.1p2 or later.
  For updates refer to http://www.openssh.com
```

Vulnerability Insight

```
The flaw exists due to an error in
  'ssh_packet_read_poll2' function within 'packet.c' script.
```

Vulnerability Detection Method

```
Get the installed version with the help
```

... continues on next page ...

... continued from previous page ...

of detect NVT and check the version is vulnerable or not.
Details:OpenSSH Denial of Service Vulnerability - Jan16
OID:1.3.6.1.4.1.25623.1.0.806671
Version used: $Revision: 4336 $

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: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105611

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

... continues on next page ...

... continued from previous page ...

cast128-cbc
rijndael-cbc@lysator.liu.se

Solution
Disable the weak encryption algorithms.

Vulnerability Insight
The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys.
The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]
↪. Arcfour (and RC4) has problems
with weak keys, and should not be used anymore.
The 'none' algorithm specifies that no encryption is to be done.
Note that this method provides no confidentiality protection, and it
is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an
↪attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details:SSH Weak Encryption Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: $Revision: 4490 $

References
Other:
URL:https://tools.ietf.org/html/rfc4253#section-6.3
URL:https://www.kb.cert.org/vuls/id/958563

Medium (CVSS: 4.3)
NVT: OpenSSH Security Bypass Vulnerability

Summary
This host is running OpenSSH and is prone
to security bypass vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.806049

Vulnerability Detection Result
Installed version: 5.1p1
Fixed version: 6.9

... continues on next page ...

... continued from previous page ...

Impact

```
Successful exploitation will allow remote
  attackers to bypass intended access restrictions.
  Impact Level: Application
```

Solution

```
Upgrade to OpenSSH version 6.9 or later.
  For updates refer to http://www.openssh.com
```

Vulnerability Insight

```
The flaw is due to the refusal
  deadline was not checked within the x11_open_helper function.
```

Vulnerability Detection Method

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

Details:`OpenSSH Security Bypass Vulnerability`
OID:`1.3.6.1.4.1.25623.1.0.806049`
Version used: `$Revision: 4336 $`

References

```
CVE: CVE-2015-5352
Other:
  URL:http://openwall.com/lists/oss-security/2015/07/01/10
```

[return to 10.0.1.101]

2.1.24 Medium 53/udp

Medium (CVSS: 6.8)
NVT: OpenSSL DSA_verify() Security Bypass Vulnerability in BIND

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.800338

... continues on next page ...

... continued from previous page ...

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.
Impact Level: Application

Solution
Upgrade to version 9.6.0 P1, 9.5.1 P1, 9.4.3 P1, 9.3.6 P1
https://www.isc.org/downloadables/11

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: 4435 $

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

Medium (CVSS: 6.8)
NVT: ISC BIND Denial of Service Vulnerability - 02 - Jan16

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.806996

... continues on next page ...

... continued from previous page ...

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.
Impact Level: Application

Solution
Upgrade to ISC BIND version 9.9.8-P3 or
9.10.3-P3 or 9.9.8-S4 or later. For updates refer to https://www.isc.org

Vulnerability Insight
The flaw is due to an error in 'apl_42.c'
script in ISC BIND.

Vulnerability Detection Method
Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:ISC BIND Denial of Service Vulnerability - 02 - Jan16
OID:1.3.6.1.4.1.25623.1.0.806996
Version used: $Revision: 4429 $

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

Summary
ISC BIND is prone to a denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.106366

... continues on next page ...

... continued from previous page ...

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
Upgrade to 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, 9.11.0-P1 or later.

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 reso
↪lver.c

Vulnerability Detection Method
Checks the version.
Details:ISC BIND Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.106366
Version used: $Revision: 4485 $

References
CVE: CVE-2016-8864
Other:
URL:https://kb.isc.org/article/AA-01434

Medium (CVSS: 5.0)
NVT: ISC BIND Denial of Service Vulnerability - 03 - Jan16

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.806997

Vulnerability Detection Result
Installed version: 9.4.2
Fixed version: 9.9.8-P2

... continues on next page ...

... continued from previous page ...

Impact

```
Successful exploitation will allow remote
  attackers to cause denial of service.
  Impact Level: Application
```

Solution

```
Upgrade to ISC BIND version 9.9.8-P2
  or 9.10.3-P2 or later.  For updates refer to https://www.isc.org
```

Vulnerability Insight

```
The flaw is due to an error in 'db.c'
  script in ISC BIND.
```

Vulnerability Detection Method

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

Details:`ISC BIND Denial of Service Vulnerability - 03 - Jan16`
OID:`1.3.6.1.4.1.25623.1.0.806997`
Version used: `$Revision: 4429 $`

References

```
CVE: CVE-2015-8000
BID:79349
Other:
  URL:https://kb.isc.org/article/AA-01317
```

Medium (CVSS: 5.0)
NVT: ISC BIND Resolver Cache Vulnerability - Jan16

Summary

```
The host is installed with ISC BIND and is
  prone to resolver cache vulnerability.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.807217

Vulnerability Detection Result

```
Installed version: 9.4.2
Fixed version:     Workaround
```

... continues on next page ...

... continued from previous page ...

Impact

```
Successful exploitation will allow remote
  attackers to trigger continued resolvability of domain names that are no
  longer registered.
  Impact Level: Application
```

Solution

```
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.
  For updates refer to https://www.isc.org
```

Vulnerability Insight

```
The flaw exist 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

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

Details:`ISC BIND Resolver Cache Vulnerability - Jan16`
OID:`1.3.6.1.4.1.25623.1.0.807217`
Version used: `$Revision: 4446 $`

References

```
CVE: CVE-2012-1033
BID:51898
Other:
  URL:https://www.kb.cert.org/vuls/id/542123
```

Medium (CVSS: 5.0)
NVT: ISC BIND NSID Request Denial of Service Vulnerability (Linux)

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.809461

... continues on next page ...

. . . continued from previous page . . .

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.
Impact Level: Application

Solution
Upgrade to ISC BIND version 9.9.9-P3 or
9.10.4-P3 or 9.11.0 or later on Linux.
For updates refer to https://www.isc.org

Vulnerability Insight
The flaw exist 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
Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:ISC BIND NSID Request Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.809461
Version used: $Revision: 4429 $

References
CVE: CVE-2016-2848
BID:93814
Other:
URL:https://kb.isc.org/article/AA-01433/74/CVE-2016-2848

Medium (CVSS: 4.3)
NVT: ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability

Summary
ISC BIND is prone to a remote denial-of-service vulnerability because
the application fails to properly handle specially crafted dynamic
update requests.

. . . continues on next page . . .

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.100251

Vulnerability Detection Result

```
OpenVAS only check 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

```
The vendor released an advisory and fixes to address this issue.
  Please see the references for more information.
```

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: 4436 $

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: 4.3)
NVT: ISC BIND lwresd Denial of Service Vulnerability

Summary

```
ISC BIND is prone to a denial of service vulnerability.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.106292

... continues on next page ...

. . . continued from previous page . . .

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
Upgrade to 9.9.9-P1, 9.10.4-P1, 9.11.0b1 or later.

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 the version.
Details:ISC BIND lwresd Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.106292
Version used: $Revision: 4429 $

References
CVE: CVE-2016-2775
Other:
URL:https://kb.isc.org/article/AA-01393

Medium (CVSS: 4.3)
NVT: ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.808751

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

Installed version: 9.4.2
Fixed version: 9.9.9-P2

Impact

Successful exploitation will allow remote
attackers to cause denial of service.
Impact Level: Application

Solution

Upgrade to ISC BIND version 9.9.9-P2 or
9.10.4-P2 or 9.11.0b2 or later. For updates refer to https://www.isc.org

Vulnerability Insight

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

Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.808751
Version used: $Revision: 4429 $

References

CVE: CVE-2016-2775
BID:92037
Other:
URL:https://kb.isc.org/article/AA-01393/74/CVE-2016-2775

Medium (CVSS: 4.0)
NVT: ISC BIND AXFR Response Denial of Service Vulnerability

Summary

ISC BIND is prone to a denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.106118

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 9.4.2
Fixed version: Workaround

Impact

An authenticated remote attacker may cause a denial of service condition.

Solution

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.

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 the version.
Details:ISC BIND AXFR Response Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.106118
Version used: $Revision: 4446 $

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

[return to 10.0.1.101]

2.1.25 Medium 53/tcp

Medium (CVSS: 6.8)
NVT: OpenSSL DSA_verify() Security Bypass Vulnerability in BIND

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.800338

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.
Impact Level: Application

Solution
Upgrade to version 9.6.0 P1, 9.5.1 P1, 9.4.3 P1, 9.3.6 P1
https://www.isc.org/downloadables/11

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: 4435 $

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

Medium (CVSS: 6.8)
NVT: ISC BIND Denial of Service Vulnerability - 02 - Jan16

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.806996

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.
  Impact Level: Application
```

Solution

```
Upgrade to ISC BIND version 9.9.8-P3 or
  9.10.3-P3 or 9.9.8-S4  or later. For updates refer to https://www.isc.org
```

Vulnerability Insight

```
The flaw is due to an error in 'apl_42.c'
  script in ISC BIND.
```

Vulnerability Detection Method

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

Details:ISC BIND Denial of Service Vulnerability - 02 - Jan16
OID:1.3.6.1.4.1.25623.1.0.806996
Version used: $Revision: 4429 $

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

Summary
ISC BIND is prone to a denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.106366

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
Upgrade to 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, 9.11.0-P1 or later.

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 reso
↪lver.c

Vulnerability Detection Method
Checks the version.
Details:ISC BIND Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.106366
Version used: $Revision: 4485 $

References
CVE: CVE-2016-8864
Other:
URL:https://kb.isc.org/article/AA-01434

Medium (CVSS: 5.0)
NVT: ISC BIND Denial of Service Vulnerability - 03 - Jan16

Summary
The host is installed with ISC BIND and is

...continues on next page ...

... continued from previous page ...

prone to remote denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.806997

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.
Impact Level: Application

Solution

Upgrade to ISC BIND version 9.9.8-P2
or 9.10.3-P2 or later. For updates refer to https://www.isc.org

Vulnerability Insight

The flaw is due to an error in 'db.c'
script in ISC BIND.

Vulnerability Detection Method

Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:ISC BIND Denial of Service Vulnerability - 03 - Jan16
OID:1.3.6.1.4.1.25623.1.0.806997
Version used: $Revision: 4429 $

References

CVE: CVE-2015-8000
BID:79349
Other:
URL:https://kb.isc.org/article/AA-01317

Medium (CVSS: 5.0)
NVT: ISC BIND Resolver Cache Vulnerability - Jan16

Summary

The host is installed with ISC BIND and is

... continues on next page ...

... continued from previous page ...

prone to resolver cache vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.807217

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.
Impact Level: Application

Solution

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.
For updates refer to https://www.isc.org

Vulnerability Insight

The flaw exist 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

Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:ISC BIND Resolver Cache Vulnerability - Jan16
OID:1.3.6.1.4.1.25623.1.0.807217
Version used: $Revision: 4446 $

References

CVE: CVE-2012-1033
BID:51898
Other:
URL:https://www.kb.cert.org/vuls/id/542123

Medium (CVSS: 5.0)
NVT: ISC BIND NSID Request Denial of Service Vulnerability (Linux)

Summary

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.809461

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.
Impact Level: Application

Solution

Upgrade to ISC BIND version 9.9.9-P3 or
9.10.4-P3 or 9.11.0 or later on Linux.
For updates refer to https://www.isc.org

Vulnerability Insight

The flaw exist 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

Get the installed version with the help
of detect NVT and check the version is vulnerable or not.
Details:ISC BIND NSID Request Denial of Service Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.809461
Version used: $Revision: 4429 $

References

CVE: CVE-2016-2848
BID:93814
Other:

. . . continues on next page . . .

... continued from previous page ...

URL:https://kb.isc.org/article/AA-01433/74/CVE-2016-2848

Medium (CVSS: 4.3)
NVT: ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability

Summary

ISC BIND is prone to a remote denial-of-service vulnerability because the application fails to properly handle specially crafted dynamic update requests.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100251

Vulnerability Detection Result

OpenVAS only check 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

The vendor released an advisory and fixes to address this issue. Please see the references for more information.

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: 4436 $

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: 4.3)
NVT: ISC BIND lwresd Denial of Service Vulnerability

Summary
ISC BIND is prone to a denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.106292

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
Upgrade to 9.9.9-P1, 9.10.4-P1, 9.11.0b1 or later.

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 the version.
Details:ISC BIND lwresd Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.106292
Version used: $Revision: 4429 $

References
CVE: CVE-2016-2775
Other:
URL:https://kb.isc.org/article/AA-01393

Medium (CVSS: 4.3)
NVT: ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability

Summary
The host is installed with ISC BIND and is

...continues on next page ...

... continued from previous page ...

prone to denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.808751

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.
Impact Level: Application

Solution

Upgrade to ISC BIND version 9.9.9-P2 or 9.10.4-P2 or 9.11.0b2 or later. For updates refer to https://www.isc.org

Vulnerability Insight

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

Get the installed version with the help of detect NVT and check the version is vulnerable or not.
Details:ISC BIND 'lightweight resolver protocol' Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.808751
Version used: $Revision: 4429 $

References

CVE: CVE-2016-2775
BID:92037
Other:
URL:https://kb.isc.org/article/AA-01393/74/CVE-2016-2775

Medium (CVSS: 4.0)
NVT: ISC BIND AXFR Response Denial of Service Vulnerability

Summary

... continues on next page ...

... continued from previous page ...

ISC BIND is prone to a denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.106118

Vulnerability Detection Result

Installed version: 9.4.2
Fixed version: Workaround

Impact

An authenticated remote attacker may cause a denial of service
condition.

Solution

As a workaround operators of servers which
  accept untrusted zone data can mitigate their risk by operating an intermediar
↪y
  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.

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 de
↪nial 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 the version.
Details:ISC BIND AXFR Response Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.106118
Version used: $Revision: 4446 $

References

CVE: CVE-2016-6170
Other:

... continues on next page ...

... continued from previous page ...

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

[return to 10.0.1.101]

2.1.26 Medium 25/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Weak Ciphers

Summary
This routine search for weak SSL/TLS ciphers offered by a service.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

Vulnerability Detection Result
'Weak' Ciphers offered by this service via the SSLv2 protocol:
SSL2_DES_192_EDE3_CBC_WITH_MD5
SSL2_DES_64_CBC_WITH_MD5
SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5
SSL2_RC2_CBC_128_CBC_WITH_MD5
SSL2_RC4_128_EXPORT40_WITH_MD5
SSL2_RC4_128_WITH_MD5
'Weak' Ciphers offered by this service via the SSLv3 protocol:
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_MD5

Solution
The configuration of this services should be changed so
that it does not support the listed weak ciphers anymore.
Please see the references for more resources supporting you with in task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2
↪protocol.
- RC4 is considered to be weak (CVE-2013-2566).
- 64-bit block cipher 3DES vulnerable to SWEET32 attack (CVE-2016-2183).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force
↪methods
and therefore considered as weak (CVE-2015-4000).

... continues on next page ...

... continued from previous page ...

```
  - 1024 bit RSA authentication is considered to be insecure and therefore as we
↪ak.
  - CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Luc
↪ky 13 attacks
  - 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 Ciphers
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: $Revision: 4614 $

References

```
CVE: CVE-2013-2566, CVE-2015-4000, CVE-2016-2183
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/
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary

The remote server's SSL/TLS certificate has already expired.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103955

Vulnerability Detection Result

```
Expired Certificates:\
\
\
The certificate on 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
```

... continues on next page ...

... continued from previous page ...

```
↪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: ED093088706603BFD5DC237399B498DA2D4D31C6
```

Solution

```
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 ex
↪pired.
```

Vulnerability Detection Method

Details:`SSL/TLS: Certificate Expired`
OID:`1.3.6.1.4.1.25623.1.0.103955`
Version used: `$Revision: 4614 $`

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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.111012

Vulnerability Detection Result

```
In addition to TLSv1+ the service is also providing the deprecated SSLv2 and SSL
↪v3 protocols and supports one or more ciphers. Those supported ciphers can be
↪found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.
```

Impact

```
An attacker might be able to use the known
  cryptographic flaws to eavesdrop the connection between clients and the servic
↪e
  to get access to sensitive data transferred within the secured connection.
```

... continues on next page ...

... continued from previous page ...

Solution
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.

Vulnerability Insight
The SSLv2 and SSLv3 protocols containing
known cryptographic flaws.

Vulnerability Detection Method
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: 4616 $

References
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/

Medium (CVSS: 4.3)
NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

Summary
This host is prone to an information disclosure vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.802087

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.
Impact Level: Application

... continues on next page ...

... continued from previous page ...

Solution
Disable SSL v3.0

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not cove
↪red by the Message Authentication Code

Vulnerability Detection Method
Send a SSLv3 request and check the response.
Details:POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: $Revision: 4161 $

References
CVE: CVE-2014-3566
BID:70574
Other:
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

Medium (CVSS: 4.3)
NVT: OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)

Summary
This host is installed with OpenSSL
and is prone to man in the middle attack.

OID of test routine: 1.3.6.1.4.1.25623.1.0.805142

Vulnerability Detection Result
EXPORT_RSA cipher suites supported by the remote server:
TLSv1.0: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014)
TLSv1.0: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0008)
TLSv1.0: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0006)
TLSv1.0: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003)

... continues on next page ...

... continued from previous page ...

Impact

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

Solution

Remove support for EXPORT_RSA cipher
suites from the service. Update to version 0.9.8zd or 1.0.0p
or 1.0.1k or later For updates refer to https://www.openssl.org

Vulnerability Insight

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

Vulnerability Detection Method

Send a crafted 'Client Hello' request
and check the servers response.
Details:OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: $Revision: 4098 $

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-f
↪actoring-nsa.html

Medium (CVSS: 4.3)
NVT: OpenSSL TLS 'DHE_EXPORT' Logjam Man in the Middle Security Bypass Vulnerability

Summary

This host is installed with OpenSSL
and is prone to man in the middle attack.

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.805188

Vulnerability Detection Result

```
DHE_EXPORT cipher suites supported by the remote server:
TLSv1.0: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0014)
```

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.
  Impact Level: Application
```

Solution

```
Remove support for DHE_EXPORT cipher
  suites from the service or Update to version 1.0.2b or 1.0.1n or later,
  For updates refer to https://www.openssl.org
```

Vulnerability Insight

```
Flaw is triggered when handling
  Diffie-Hellman key exchanges defined in the DHE_EXPORT cipher
```

Vulnerability Detection Method

```
Send a crafted 'Client Hello' request
  and check the servers response.
```

Details:OpenSSL TLS 'DHE_EXPORT' LogJam Man in the Middle Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.805188
Version used: $Revision: 4098 $

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: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary

The remote service is using a SSL/TLS certificate chain that has been signed usi
↪ng a cryptographically weak hashing algorithm.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105880

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

Vulnerability Insight

Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not sec
↪ure enough for ongoing use. Beginning as late as January 2017
and as early as June 2016, browser developers such as Microsoft and Google wil
↪l begin warning users when users visit web sites that use SHA-1 signed Secure
↪Socket Layer (SSL)
certificates. Servers that use SSL/TLS certificates signed using an SHA-1 sign
↪ature will need to obtain new SHA-2 signed SSL/TLS certificates to avoid these
↪ web browser SSL/TLS certificate warnings.

Vulnerability Detection Method

Check which 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: 4614 $

References

Other:
URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
↪-sha-1-based-signature-algorithms/

. . . continues on next page . . .

... continued from previous page ...

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).

OID of test routine: 1.3.6.1.4.1.25623.1.0.106223

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits\

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.
↪html)

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 fi
↪nal 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 Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: $Revision: 4614 $

References
Other:
URL:https://weakdh.org/

[return to 10.0.1.101]

2.1.27 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

Vulnerability Detection Result

It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 725551
Paket 2: 725665

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

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 timesta
↪mps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be complete
↪ly 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 pee
↪r
that is initiating communication includes them in their synchronize (SYN) segm
↪ent.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

... continues on next page ...

. . . continued from previous page . . .

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 timestam
↪ps are reported.
```

Details:`TCP timestamps`

OID:`1.3.6.1.4.1.25623.1.0.80091`

Version used: `$Revision: 4408 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

[return to 10.0.1.101]

2.1.28 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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900841

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.
  Impact Level: Application
```

Solution

```
Upgrade to Apache HTTP Server version 2.2.15 or later
  For updates refer to http://www.apache.org/
```

Vulnerability Insight

```
The flaw is due to an error in 'ap_proxy_ftp_handler' function in
```

. . . continues on next page . . .

... continued from previous page ...

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: 3386 $

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

Low (CVSS: 2.1)
NVT: PHP 'mbstring.func_overload' DoS Vulnerability

Summary
The host is running PHP and is prone to denial of service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.800373

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 se
↪rver.
Impact Level: Application

Solution
Apply patch from below link,
http://php.net

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

```
This bug is due to an error in 'mbstring.func_overload' setting in .htaccess
  file. It can be exploited via modifying behavior of other sites hosted on
  the same web server which causes this setting to be applied to other virtual
  hosts on the same server.
```

Vulnerability Detection Method

Details:PHP 'mbstring.func_overload' DoS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800373
Version used: $Revision: 4504 $

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
```

[return to 10.0.1.101]

2.1.29 Low 445/tcp

Low (CVSS: 3.3)
NVT: Samba 'etc/mtab' File Appending Local Denial of Service Vulnerability

Summary

```
Samba is prone to a local denial-of-service vulnerability.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103298

Vulnerability Detection Result

```
Installed version: 3.0.20
Fixed version:     3.5.9
```

Impact

```
A local attacker can exploit this issue to cause the computer to stop
  responding, denying service to legitimate users.
```

... continues on next page ...

... continued from previous page ...

Solution
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: 4398 $

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: 2.1)
NVT: Samba 'client/mount.cifs.c' Remote Denial of Service Vulnerability

Summary
Samba is prone to a remote denial-of-service vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100499

Vulnerability Detection Result
Installed version: 3.0.20
Fixed version: 3.5.11 or later

Impact
A remote attacker can exploit this issue to crash the affected
application, denying service to legitimate users.

Solution
Upgrade to Samba version 3.5.11 or later.

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

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 4387 $

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
↪fafeebb2e054
   URL:http://us1.samba.org/samba/
```

[return to 10.0.1.101]

2.1.30 Low 3306/tcp

Low (CVSS: 3.5)
NVT: MySQL 'ALTER DATABASE' Remote Denial Of Service Vulnerability

Summary

```
The host is running MySQL and is prone to Denial Of Service
  vulnerability.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.801380

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.
  Impact Level: Application
```

Solution

```
Upgrade to MySQL version 5.1.48
  For updates refer to http://dev.mysql.com/downloads
```

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 '..'.
```

... continues on next page ...

... continued from previous page ...

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: 3152 $

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

[return to 10.0.1.101]

2.1.31 Low 5432/tcp

Low (CVSS: 3.5)
NVT: PostgreSQL Hash Table Integer Overflow Vulnerability

Summary
The host is running PostgreSQL and is prone to integer overflow vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.902139

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

Impact
Successful exploitation could allow execution of specially-crafted sql query which once processed would lead to denial of service (postgresql daemon crash)
↪.
Impact Level: Application

Solution

... continues on next page ...

... continued from previous page ...

```
Apply the patch,
  http://git.postgresql.org/gitweb?p=postgresql.git
a=commitdiff
h=64b057e6823655fb6c5d1f24a28f236b94dd6c54
  ******
  NOTE: Please ignore this warning if the patch is applied.
  ******
```

Vulnerability Insight

```
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: 3184 $

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
```

Low (CVSS: 2.1)
NVT: PostgreSQL Low Cost Function Information Disclosure Vulnerability

Summary

```
PostgreSQL is prone to an information-disclosure vulnerability.
  Local attackers can exploit this issue to obtain sensitive
  information that may lead to further attacks.
  PostgreSQL 8.3.6 is vulnerable
 other versions may also be affected.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100158

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

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: 3911 $

References
BID:34069
Other:
URL:http://www.securityfocus.com/bid/34069
URL:http://www.postgresql.org/

[return to 10.0.1.101]

2.1.32 Low 22/tcp

Low (CVSS: 3.5)
NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability

Summary
The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103503

Vulnerability Detection Result
According to its banner, the version of OpenSSH installed on the remote host is older than 5.7:
SSH-2.0-OpenSSH_5.1p1 Debian-5ubuntu1

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details:openssh-server Forced Command Handling Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103503
Version used: $Revision: 4336 $

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: 3.5)
NVT: OpenSSH 'ssh_gssapi_parse_ename()' Function Denial of Service Vulnerability

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.103937

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

Impact
Exploiting this issue allows remote attackers to trigger
denial-of-service conditions due to excessive memory consumption.

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Check the version.
Details:OpenSSH 'ssh_gssapi_parse_ename()' Function Denial of Service Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103937
Version used: $Revision: 4336 $

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2011-5000
BID:54114
Other:
URL:http://www.securityfocus.com/bid/54114
URL:http://www.openssh.com

Low (CVSS: 2.6)
NVT: OpenSSH CBC Mode Information Disclosure Vulnerability

Summary
The host is installed with OpenSSH and is prone to information disclosure vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100153

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

Impact
Successful exploits will allow attackers to obtain four bytes of plaintext from an encrypted session.
Impact Level: Application

Solution
Upgrade to higher version
http://www.openssh.com/portable.html

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: 3445 $

... continues on next page ...

. . . continued from previous page . . .

References
CVE: CVE-2008-5161
BID:32319
Other:
URL:http://www.securityfocus.com/bid/32319

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 algorith
↪ms.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105610

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
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details:SSH Weak MAC Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: $Revision: 4490 $

Low (CVSS: 2.1)
NVT: OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability

Summary

. . . continues on next page . . .

... continued from previous page ...

OpenSSH is prone to a local information-disclosure vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105002

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

Impact
Local attackers can exploit this issue to obtain sensitive information. Information obtained may lead to further attacks.

Solution
Updates are available.

Vulnerability Insight
ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.

Vulnerability Detection Method
Check the version.
Details:OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105002
Version used: $Revision: 4336 $

References
CVE: CVE-2011-4327
BID:65674
Other:
URL:http://www.securityfocus.com/bid/65674
URL:http://www.openssh.com
URL:http://www.openssh.com/txt/portable-keysign-rand-helper.adv

[return to 10.0.1.101]

2.1.33 Low 53/udp

Low (CVSS: 2.6)
NVT: ISC BIND 9 DNSSEC Query Response Additional Section Remote Cache Poisoning Vulnerability

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100362

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
Updates are available. Please see the references for details.

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: 4435 $

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 10.0.1.101]

2.1.34 Low 53/tcp

Low (CVSS: 2.6)
NVT: ISC BIND 9 DNSSEC Query Response Additional Section Remote Cache Poisoning Vulnerability

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100362

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
Updates are available. Please see the references for details.

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: 4435 $

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 10.0.1.101]

2.1.35 Log general/tcp

Log (CVSS: 0.0)
NVT: Nmap OS Identification (NASL wrapper)

Summary
This plugin runs nmap to identify the remote Operating System.

OID of test routine: 1.3.6.1.4.1.25623.1.0.108021

Vulnerability Detection Result
Detected OS: Linux 2.6.9 - 2.6.33
CPE: cpe:/o:linux:linux_kernel:2.6
Concluded from Nmap TCP/IP fingerprinting :
OS details: Linux 2.6.9 - 2.6.33
OS CPE: cpe:/o:linux:linux_kernel:2.6

Log Method
Details:Nmap OS Identification (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.108021
Version used: $Revision: 4580 $

References
Other:
URL:https://nmap.org/book/man-os-detection.html
URL:https://nmap.org/book/osdetect.html

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
Here is the route from 10.0.1.102 to 10.0.1.101:
10.0.1.102
10.0.1.101
```

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: 4048 $`

[return to 10.0.1.101]

2.1.36 Log 8787/tcp

Log (CVSS: 0.0)
NVT: Identify unknown services with GET

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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.17975

Vulnerability Detection Result

```
A Distributed Ruby (dRuby/DRb) service seems to be running on this port.
```

Log Method

Details:`Identify unknown services with GET`
OID:`1.3.6.1.4.1.25623.1.0.17975`
Version used: `$Revision: 4381 $`

[return to 10.0.1.101]

2.1.37 Log 80/tcp

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This detects the HTTP Server's type and version.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10107

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
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: 3564 $

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

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: 3923 $

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.1
↪1032)
- Various OS fingerprinting methods
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan confi
↪g in use

OID of test routine: 1.3.6.1.4.1.25623.1.0.111038

Vulnerability Detection Result
The host seems to be running on a Unix-like operating system.
The host seems to be able to host PHP scripts.
The host seems to be NOT able to host ASP scripts.
The following directories require authentication and are tested by the script \"
↪HTTP Brute Force Logins with default Credentials (OID: 1.3.6.1.4.1.25623.1.0.1
↪03240)\":
http://10.0.1.101/twiki/pub/TWiki/TWikiLogos/
The following directories were used for CGI scanning:
http://10.0.1.101/
http://10.0.1.101/cgi-bin
http://10.0.1.101/dav
http://10.0.1.101/doc
http://10.0.1.101/dvwa
http://10.0.1.101/icons
http://10.0.1.101/mutillidae
http://10.0.1.101/mutillidae/documentation
http://10.0.1.101/mutillidae/images
http://10.0.1.101/mutillidae/javascript
http://10.0.1.101/mutillidae/javascript/ddsmoothmenu
http://10.0.1.101/mutillidae/styles

... continues on next page ...

... continued from previous page ...

```
http://10.0.1.101/mutillidae/styles/ddsmoothmenu
http://10.0.1.101/oops/TWiki
http://10.0.1.101/phpMyAdmin
http://10.0.1.101/phpMyAdmin/themes/original
http://10.0.1.101/phpMyAdmin/themes/original/img
http://10.0.1.101/rdiff/TWiki
http://10.0.1.101/scripts
http://10.0.1.101/test
http://10.0.1.101/test/testoutput
http://10.0.1.101/twiki
http://10.0.1.101/twiki/pub
http://10.0.1.101/twiki/pub/TWiki/FileAttachment
http://10.0.1.101/twiki/pub/TWiki/TWikiDocGraphics
http://10.0.1.101/twiki/pub/TWiki/TWikiLogos
http://10.0.1.101/twiki/pub/TWiki/TWikiPreferences
http://10.0.1.101/twiki/pub/TWiki/TWikiTemplates
http://10.0.1.101/twiki/pub/icn
http://10.0.1.101/view/TWiki
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
Directory index found at:
http://10.0.1.101/dav/
http://10.0.1.101/mutillidae/documentation/
http://10.0.1.101/mutillidae/images/
http://10.0.1.101/mutillidae/javascript/
http://10.0.1.101/mutillidae/javascript/ddsmoothmenu/
http://10.0.1.101/mutillidae/styles/
http://10.0.1.101/mutillidae/styles/ddsmoothmenu/
http://10.0.1.101/phpMyAdmin/themes/original/img/
http://10.0.1.101/test/
http://10.0.1.101/test/testoutput/
http://10.0.1.101/twiki/TWikiDocumentation.html
http://10.0.1.101/twiki/bin/view/TWiki/TWikiDocumentation
http://10.0.1.101/twiki/bin/view/TWiki/TWikiInstallationGuide
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://10.0.1.101/dav/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://10.0.1.101/mutillidae/ (page [add-to-your-blog.php] )
http://10.0.1.101/mutillidae/documentation/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O
↪ [A] )
http://10.0.1.101/mutillidae/images/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://10.0.1.101/mutillidae/index.php (username [anonymous] do [toggle-hints] p
↪age [home.php] )
http://10.0.1.101/mutillidae/javascript/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A
↪] )
http://10.0.1.101/mutillidae/javascript/ddsmoothmenu/ (C=S;O [A] C=N;O [D] C=M;O
```

... continues on next page ...

... continued from previous page ...

```
↪ [A] C=D;O [A] )
http://10.0.1.101/mutillidae/styles/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://10.0.1.101/mutillidae/styles/ddsmoothmenu/ (C=S;O [A] C=N;O [D] C=M;O [A]
↪ C=D;O [A] )
http://10.0.1.101/oops/TWiki/TWikiHistory (template [oopsrev] param1 [1.10] )
http://10.0.1.101/phpMyAdmin/index.php (phpMyAdmin [676164c887302620e8943b01cfb7
↪cf813bba0bcf] token [030fa6ef0c5cb8872ad3962b1bc1b24f] pma_username [] table [
↪] lang [] server [1] db [] convcharset [utf-8] pma_password [] )
http://10.0.1.101/phpMyAdmin/phpmyadmin.css.php (token [030fa6ef0c5cb8872ad3962b
↪1bc1b24f] js_frame [right] lang [en-utf-8] nocache [2457687151] convcharset [u
↪tf-8] )
http://10.0.1.101/phpMyAdmin/themes/original/img/ (C=S;O [A] C=N;O [D] C=M;O [A]
↪ C=D;O [A] )
http://10.0.1.101/rdiff/TWiki/TWikiHistory (rev1 [1.10] rev2 [1.9] )
http://10.0.1.101/test/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://10.0.1.101/test/testoutput/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://10.0.1.101/twiki/bin/attach/TWiki/FileAttachment (filename [Sample.txt] r
↪evInfo [1] )
http://10.0.1.101/twiki/bin/edit/Know/WebChanges (t [1481267213] )
http://10.0.1.101/twiki/bin/edit/Know/WebHome (t [1481267086] )
http://10.0.1.101/twiki/bin/edit/Know/WebPreferences (t [1481267225] )
http://10.0.1.101/twiki/bin/edit/Know/WebSearch (t [1481267223] )
http://10.0.1.101/twiki/bin/edit/Main/EngineeringGroup (topicparent [Main.TWikiG
↪roups] )
http://10.0.1.101/twiki/bin/edit/Main/GoodStyle (topicparent [Main.WebHome] )
http://10.0.1.101/twiki/bin/edit/Main/MartinRaabe (topicparent [TWiki.TWikiUpgra
↪deGuide] )
http://10.0.1.101/twiki/bin/edit/Main/OfficeLocations (t [1481267135] )
http://10.0.1.101/twiki/bin/edit/Main/PeterThoeny (t [1481267369] )
http://10.0.1.101/twiki/bin/edit/Main/SupportGroup (topicparent [Main.TWikiGroup
↪s] )
http://10.0.1.101/twiki/bin/edit/Main/TWikiGroups (t [1481267132] )
http://10.0.1.101/twiki/bin/edit/Main/TWikiPreferences (topicparent [Main.WebHom
↪e] )
http://10.0.1.101/twiki/bin/edit/Main/TWikiUsers (t [1481267129] )
http://10.0.1.101/twiki/bin/edit/Main/TWikiWeb (topicparent [Main.WebHome] )
http://10.0.1.101/twiki/bin/edit/Main/TestArea (topicparent [Main.WebHome] )
http://10.0.1.101/twiki/bin/edit/Main/TextFormattingFAQ (topicparent [Main.WebHo
↪me] )
http://10.0.1.101/twiki/bin/edit/Main/TextFormattingRules (topicparent [Main.Web
↪Home] )
http://10.0.1.101/twiki/bin/edit/Main/WebChanges (t [1481267137] )
http://10.0.1.101/twiki/bin/edit/Main/WebHome (t [1481266952] )
http://10.0.1.101/twiki/bin/edit/Main/WebIndex (t [1481267158] )
http://10.0.1.101/twiki/bin/edit/Main/WebNotify (t [1481267254] )
http://10.0.1.101/twiki/bin/edit/Main/WebPreferences (t [1481267178] )
http://10.0.1.101/twiki/bin/edit/Main/WebSearch (t [1481267165] )
```

... continues on next page ...

... continued from previous page ...

```
http://10.0.1.101/twiki/bin/edit/Main/WebStatistics (t [1481267258] )
http://10.0.1.101/twiki/bin/edit/Main/WebTopicEditTemplate (topicparent [Main.We
↪bPreferences] )
http://10.0.1.101/twiki/bin/edit/Main/WebTopicList (t [1481267249] )
http://10.0.1.101/twiki/bin/edit/Main/WelcomeGuest (topicparent [Main.WebHome] )
http://10.0.1.101/twiki/bin/edit/Sandbox/TestTopic1 (topicparent [Sandbox.WebHom
↪e] )
http://10.0.1.101/twiki/bin/edit/Sandbox/TestTopic2 (topicparent [Sandbox.WebHom
↪e] )
http://10.0.1.101/twiki/bin/edit/Sandbox/TestTopic3 (topicparent [Sandbox.WebHom
↪e] )
http://10.0.1.101/twiki/bin/edit/Sandbox/TestTopic4 (topicparent [Sandbox.WebHom
↪e] )
http://10.0.1.101/twiki/bin/edit/Sandbox/TestTopic5 (topicparent [Sandbox.WebHom
↪e] )
http://10.0.1.101/twiki/bin/edit/Sandbox/TestTopic6 (topicparent [Sandbox.WebHom
↪e] )
http://10.0.1.101/twiki/bin/edit/Sandbox/TestTopic7 (topicparent [Sandbox.WebHom
↪e] )
http://10.0.1.101/twiki/bin/edit/Sandbox/TestTopic8 (topicparent [Sandbox.WebHom
↪e] )
http://10.0.1.101/twiki/bin/edit/Sandbox/WebChanges (t [1481267227] )
http://10.0.1.101/twiki/bin/edit/Sandbox/WebHome (t [1481267108] )
http://10.0.1.101/twiki/bin/edit/Sandbox/WebPreferences (t [1481267243] )
http://10.0.1.101/twiki/bin/edit/Sandbox/WebSearch (t [1481267237] )
http://10.0.1.101/twiki/bin/edit/Sandbox/WebTopicEditTemplate (topicparent [Sand
↪box.WebPreferences] )
http://10.0.1.101/twiki/bin/edit/TWiki/ (topic [] topicparent [TWikiFAQ] onlywik
↪iname [on] templatetopic [TWikiFaqTemplate] )
http://10.0.1.101/twiki/bin/edit/TWiki/AppendixFileSystem (t [1481267510] )
http://10.0.1.101/twiki/bin/edit/TWiki/DefaultPlugin (t [1481267413] )
http://10.0.1.101/twiki/bin/edit/TWiki/FileAttachment (t [1481267402] )
http://10.0.1.101/twiki/bin/edit/TWiki/FormattedSearch (t [1481267468] )
http://10.0.1.101/twiki/bin/edit/TWiki/GnuGeneralPublicLicense (t [1481267524] )
http://10.0.1.101/twiki/bin/edit/TWiki/GoodStyle (t [1481267347] )
http://10.0.1.101/twiki/bin/edit/TWiki/InstalledPlugins (t [1481267520] )
http://10.0.1.101/twiki/bin/edit/TWiki/InstantEnhancements (t [1481267423] )
http://10.0.1.101/twiki/bin/edit/TWiki/InterWikis (t [1481267416] )
http://10.0.1.101/twiki/bin/edit/TWiki/InterwikiPlugin (t [1481267415] )
http://10.0.1.101/twiki/bin/edit/TWiki/ManagingTopics (t [1481267502] )
http://10.0.1.101/twiki/bin/edit/TWiki/ManagingWebs (t [1481267507] )
http://10.0.1.101/twiki/bin/edit/TWiki/MeaningfulTitle (topicparent [TWiki.TextF
↪ormattingFAQ] )
http://10.0.1.101/twiki/bin/edit/TWiki/NewTopic (topicparent [TWiki.TWikiShortha
↪nd] )
http://10.0.1.101/twiki/bin/edit/TWiki/NotExistingYet (topicparent [TWiki.TextFo
↪rmattingRules] )
```

... continues on next page ...

... continued from previous page ...

```
http://10.0.1.101/twiki/bin/edit/TWiki/PeterThoeny (t [1481267523] )
http://10.0.1.101/twiki/bin/edit/TWiki/SiteMap (t [1481267521] )
http://10.0.1.101/twiki/bin/edit/TWiki/StartingPoints (t [1481267186] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiAccessControl (t [1481267453] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiAdminCookBook (t [1481267418] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiCourseOutlineExample (topicparent [T
↪Wiki.WebHome] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiFAQ (t [1481267272] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiForms (t [1481267206] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiFuncModule (t [1481267485] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiGlossary (t [1481267411] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiHistory (t [1481267337] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiImplementationNotes (topicparent [TW
↪iki.WebHome] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiInstallationGuide (t [1481267429] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiMetaData (t [1481267472] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiPlugins (t [1481267478] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiPreferences (t [1481267264] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiRegistration (t [1481267183] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiShorthand (t [1481267397] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiSite (t [1481267270] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiSiteTools (t [1481267499] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiSkins (t [1481267464] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiSystemRequirements (t [1481267427] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiTemplates (t [1481267458] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiTopic (topicparent [TWiki.TWikiTopic
↪s] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiTopics (t [1481267394] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiTutorial (t [1481267391] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiUpgradeGuide (t [1481267446] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiUserAuthentication (t [1481267450] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiVariables (t [1481267399] )
http://10.0.1.101/twiki/bin/edit/TWiki/TWikiWeb (topicparent [Main.WebHome] )
http://10.0.1.101/twiki/bin/edit/TWiki/TextFormattingFAQ (t [1481267357] )
http://10.0.1.101/twiki/bin/edit/TWiki/TextFormattingRules (t [1481267349] )
http://10.0.1.101/twiki/bin/edit/TWiki/WebChanges (t [1481267188] )
http://10.0.1.101/twiki/bin/edit/TWiki/WebChangesAlert (t [1481267409] )
http://10.0.1.101/twiki/bin/edit/TWiki/WebHome (t [1481267022] )
http://10.0.1.101/twiki/bin/edit/TWiki/WebIndex (t [1481267377] )
http://10.0.1.101/twiki/bin/edit/TWiki/WebNotify (t [1481267517] )
http://10.0.1.101/twiki/bin/edit/TWiki/WebPreferences (t [1481267205] )
http://10.0.1.101/twiki/bin/edit/TWiki/WebSearch (t [1481267203] )
http://10.0.1.101/twiki/bin/edit/TWiki/WebStatistics (t [1481267518] )
http://10.0.1.101/twiki/bin/edit/TWiki/WebTopicList (t [1481267371] )
http://10.0.1.101/twiki/bin/edit/TWiki/WelcomeGuest (t [1481267172] )
http://10.0.1.101/twiki/bin/edit/TWiki/WikiOrg (topicparent [TWiki.TWikiAdminCoo
↪kBook] )
```

... continues on next page ...

. . . continued from previous page . . .

```
http://10.0.1.101/twiki/bin/edit/TWiki/WikiStyleWord (topicparent [TWiki.TextFor
↪mattingFAQ] )
http://10.0.1.101/twiki/bin/edit/TWiki/WindowsInstallCookbook (t [1481267435] )
http://10.0.1.101/twiki/bin/manage/TWiki/ManagingWebs (newweb [] baseweb [] webb
↪gcolor [#D0D0D0] sitemapwhat [] sitemapuseto [...collaborate on] nosearchall [
↪] nosearchall [on] newtopic [] action [createweb] )
http://10.0.1.101/twiki/bin/oops/Know/WebChanges (template [oopsmore] param1 [1.
↪2] param2 [1.2] )
http://10.0.1.101/twiki/bin/oops/Know/WebHome (template [oopsmore] param1 [1.10]
↪ param2 [1.10] )
http://10.0.1.101/twiki/bin/oops/Know/WebPreferences (template [oopsmore] param1
↪ [1.11] param2 [1.11] )
http://10.0.1.101/twiki/bin/oops/Know/WebSearch (template [oopsmore] param1 [1.9
↪] param2 [1.9] )
http://10.0.1.101/twiki/bin/oops/Main/OfficeLocations (template [oopsmore] param
↪1 [1.4] param2 [1.4] )
http://10.0.1.101/twiki/bin/oops/Main/PeterThoeny (template [oopsmore] param1 [1
↪.8] param2 [1.8] )
http://10.0.1.101/twiki/bin/oops/Main/TWikiGroups (template [oopsmore] param1 [1
↪.3] param2 [1.3] )
http://10.0.1.101/twiki/bin/oops/Main/TWikiUsers (template [oopsmore] param1 [1.
↪16] param2 [1.16] )
http://10.0.1.101/twiki/bin/oops/Main/WebChanges (template [oopsmore] param1 [1.
↪2] param2 [1.2] )
http://10.0.1.101/twiki/bin/oops/Main/WebHome (param1 [1.20] param2 [1.20] templ
↪ate [oopsmore] )
http://10.0.1.101/twiki/bin/oops/Main/WebIndex (template [oopsmore] param1 [1.2]
↪ param2 [1.2] )
http://10.0.1.101/twiki/bin/oops/Main/WebNotify (template [oopsmore] param1 [1.7
↪] param2 [1.7] )
http://10.0.1.101/twiki/bin/oops/Main/WebPreferences (template [oopsmore] param1
↪ [1.13] param2 [1.13] )
http://10.0.1.101/twiki/bin/oops/Main/WebSearch (template [oopsmore] param1 [1.8
↪] param2 [1.8] )
http://10.0.1.101/twiki/bin/oops/Main/WebStatistics (template [oopsmore] param1
↪[1.4] param2 [1.4] )
http://10.0.1.101/twiki/bin/oops/Main/WebTopicList (template [oopsmore] param1 [
↪1.1] param2 [1.1] )
http://10.0.1.101/twiki/bin/oops/Sandbox/WebChanges (template [oopsmore] param1
↪[1.2] param2 [1.2] )
http://10.0.1.101/twiki/bin/oops/Sandbox/WebHome (template [oopsmore] param1 [1.
↪7] param2 [1.7] )
http://10.0.1.101/twiki/bin/oops/Sandbox/WebPreferences (template [oopsmore] par
↪am1 [1.10] param2 [1.10] )
http://10.0.1.101/twiki/bin/oops/Sandbox/WebSearch (template [oopsmore] param1 [
↪1.6] param2 [1.6] )
http://10.0.1.101/twiki/bin/oops/TWiki/AppendixFileSystem (template [oopsmore] p
```

. . . continues on next page . . .

... continued from previous page ...

```
↪aram1 [1.12] param2 [1.12] )
http://10.0.1.101/twiki/bin/oops/TWiki/DefaultPlugin (template [oopsmore] param1
↪ [1.5] param2 [1.5] )
http://10.0.1.101/twiki/bin/oops/TWiki/FileAttachment (template [oopsmore] param
↪1 [1.10] param2 [1.10] )
http://10.0.1.101/twiki/bin/oops/TWiki/FormattedSearch (template [oopsmore] para
↪m1 [1.9] param2 [1.9] )
http://10.0.1.101/twiki/bin/oops/TWiki/GnuGeneralPublicLicense (template [oopsmo
↪re] param1 [1.2] param2 [1.2] )
http://10.0.1.101/twiki/bin/oops/TWiki/GoodStyle (template [oopsmore] param1 [1.
↪6] param2 [1.6] )
http://10.0.1.101/twiki/bin/oops/TWiki/InstalledPlugins (template [oopsmore] par
↪am1 [1.1] param2 [1.1] )
http://10.0.1.101/twiki/bin/oops/TWiki/InstantEnhancements (template [oopsmore]
↪param1 [1.1] param2 [1.1] )
http://10.0.1.101/twiki/bin/oops/TWiki/InterWikis (template [oopsmore] param1 [1
↪.3] param2 [1.3] )
http://10.0.1.101/twiki/bin/oops/TWiki/InterwikiPlugin (template [oopsmore] para
↪m1 [1.6] param2 [1.6] )
http://10.0.1.101/twiki/bin/oops/TWiki/ManagingTopics (template [oopsmore] param
↪1 [1.17] param2 [1.17] )
http://10.0.1.101/twiki/bin/oops/TWiki/ManagingWebs (template [oopsmore] param1
↪[1.23] param2 [1.23] )
http://10.0.1.101/twiki/bin/oops/TWiki/PeterThoeny (template [oopsmore] param1 [
↪1.4] param2 [1.4] )
http://10.0.1.101/twiki/bin/oops/TWiki/SiteMap (template [oopsmore] param1 [1.2]
↪ param2 [1.2] )
http://10.0.1.101/twiki/bin/oops/TWiki/StartingPoints (template [oopsmore] param
↪1 [1.3] param2 [1.3] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiAccessControl (template [oopsmore] p
↪aram1 [1.27] param2 [1.27] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiAdminCookBook (template [oopsmore] p
↪aram1 [1.2] param2 [1.2] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiFAQ (template [oopsmore] param1 [1.1
↪2] param2 [1.12] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiForms (template [oopsmore] param1 [1
↪.16] param2 [1.16] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiFuncModule (template [oopsmore] para
↪m1 [1.3] param2 [1.3] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiGlossary (template [oopsmore] param1
↪ [1.2] param2 [1.2] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiHistory (param1 [1.10] param2 [1.61]
↪ template [oopsrev] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiInstallationGuide (template [oopsmor
↪e] param1 [1.53] param2 [1.53] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiMetaData (template [oopsmore] param1
↪ [1.11] param2 [1.11] )
```

... continues on next page ...

... continued from previous page ...

```
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiPlugins (template [oopsmore] param1
↪[1.21] param2 [1.21] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiPreferences (template [oopsmore] par
↪am1 [1.47] param2 [1.47] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiRegistration (template [oopsmore] pa
↪ram1 [1.8] param2 [1.8] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiShorthand (template [oopsmore] param
↪1 [1.1] param2 [1.1] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiSite (template [oopsmore] param1 [1.
↪21] param2 [1.21] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiSiteTools (template [oopsmore] param
↪1 [1.7] param2 [1.7] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiSkins (template [oopsmore] param1 [1
↪.11] param2 [1.11] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiSystemRequirements (template [oopsmo
↪re] param1 [1.28] param2 [1.28] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiTemplates (template [oopsmore] param
↪1 [1.18] param2 [1.18] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiTopics (template [oopsmore] param1 [
↪1.12] param2 [1.12] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiTutorial (template [oopsmore] param1
↪ [1.12] param2 [1.12] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiUpgradeGuide (template [oopsmore] pa
↪ram1 [1.3] param2 [1.3] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiUserAuthentication (template [oopsmo
↪re] param1 [1.15] param2 [1.15] )
http://10.0.1.101/twiki/bin/oops/TWiki/TWikiVariables (template [oopsmore] param
↪1 [1.62] param2 [1.62] )
http://10.0.1.101/twiki/bin/oops/TWiki/TextFormattingFAQ (template [oopsmore] pa
↪ram1 [1.14] param2 [1.14] )
http://10.0.1.101/twiki/bin/oops/TWiki/TextFormattingRules (template [oopsmore]
↪param1 [1.37] param2 [1.37] )
http://10.0.1.101/twiki/bin/oops/TWiki/WebChanges (template [oopsmore] param1 [1
↪.3] param2 [1.3] )
http://10.0.1.101/twiki/bin/oops/TWiki/WebChangesAlert (template [oopsmore] para
↪m1 [1.13] param2 [1.13] )
http://10.0.1.101/twiki/bin/oops/TWiki/WebHome (param1 [1.78] param2 [1.78] temp
↪late [oopsmore] )
http://10.0.1.101/twiki/bin/oops/TWiki/WebIndex (template [oopsmore] param1 [1.2
↪] param2 [1.2] )
http://10.0.1.101/twiki/bin/oops/TWiki/WebNotify (template [oopsmore] param1 [1.
↪5] param2 [1.5] )
http://10.0.1.101/twiki/bin/oops/TWiki/WebPreferences (template [oopsmore] param
↪1 [1.17] param2 [1.17] )
http://10.0.1.101/twiki/bin/oops/TWiki/WebSearch (template [oopsmore] param1 [1.
↪12] param2 [1.12] )
http://10.0.1.101/twiki/bin/oops/TWiki/WebStatistics (template [oopsmore] param1
```

... continues on next page ...

... continued from previous page ...

```
↪ [1.3] param2 [1.3] )
http://10.0.1.101/twiki/bin/oops/TWiki/WebTopicList (template [oopsmore] param1
↪[1.1] param2 [1.1] )
http://10.0.1.101/twiki/bin/oops/TWiki/WelcomeGuest (template [oopsmore] param1
↪[1.20] param2 [1.20] )
http://10.0.1.101/twiki/bin/oops/TWiki/WindowsInstallCookbook (template [oopsmor
↪e] param1 [1.3] param2 [1.3] )
http://10.0.1.101/twiki/bin/passwd/Main/WebHome (username [] password [] passwor
↪dA [] TopicName [ResetPassword] )
http://10.0.1.101/twiki/bin/passwd/TWiki/WebHome (username [] oldpassword [] pas
↪sword [] passwordA [] TopicName [ChangePassword] change [on] )
http://10.0.1.101/twiki/bin/preview/Main/WebHome (formtemplate [] topicparent []
↪ cmd [] )
http://10.0.1.101/twiki/bin/preview/TWiki/WebHome (formtemplate [] topicparent [
↪] cmd [] )
http://10.0.1.101/twiki/bin/rdiff/Know/WebChanges (rev1 [1.2] rev2 [1.1] )
http://10.0.1.101/twiki/bin/rdiff/Know/WebHome (rev1 [1.10] rev2 [1.9] )
http://10.0.1.101/twiki/bin/rdiff/Know/WebPreferences (rev1 [1.11] rev2 [1.10] )
http://10.0.1.101/twiki/bin/rdiff/Know/WebSearch (rev1 [1.9] rev2 [1.8] )
http://10.0.1.101/twiki/bin/rdiff/Main/OfficeLocations (rev1 [1.4] rev2 [1.3] )
http://10.0.1.101/twiki/bin/rdiff/Main/PeterThoeny (rev1 [1.8] rev2 [1.7] )
http://10.0.1.101/twiki/bin/rdiff/Main/TWikiGroups (rev1 [1.3] rev2 [1.2] )
http://10.0.1.101/twiki/bin/rdiff/Main/TWikiUsers (rev1 [1.16] rev2 [1.15] )
http://10.0.1.101/twiki/bin/rdiff/Main/WebChanges (rev1 [1.2] rev2 [1.1] )
http://10.0.1.101/twiki/bin/rdiff/Main/WebHome (rev1 [1.20] rev2 [1.19] )
http://10.0.1.101/twiki/bin/rdiff/Main/WebIndex (rev1 [1.2] rev2 [1.1] )
http://10.0.1.101/twiki/bin/rdiff/Main/WebNotify (rev1 [1.7] rev2 [1.6] )
http://10.0.1.101/twiki/bin/rdiff/Main/WebPreferences (rev1 [1.13] rev2 [1.12] )
http://10.0.1.101/twiki/bin/rdiff/Main/WebSearch (rev1 [1.8] rev2 [1.7] )
http://10.0.1.101/twiki/bin/rdiff/Main/WebStatistics (rev1 [1.4] rev2 [1.3] )
http://10.0.1.101/twiki/bin/rdiff/Sandbox/WebChanges (rev1 [1.2] rev2 [1.1] )
http://10.0.1.101/twiki/bin/rdiff/Sandbox/WebHome (rev1 [1.7] rev2 [1.6] )
http://10.0.1.101/twiki/bin/rdiff/Sandbox/WebPreferences (rev1 [1.10] rev2 [1.9]
↪ )
http://10.0.1.101/twiki/bin/rdiff/Sandbox/WebSearch (rev1 [1.6] rev2 [1.5] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/AppendixFileSystem (rev1 [1.12] rev2 [1.
↪11] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/DefaultPlugin (rev1 [1.5] rev2 [1.4] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/FileAttachment (rev1 [1.10] rev2 [1.9] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/FormattedSearch (rev1 [1.9] rev2 [1.8] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/GnuGeneralPublicLicense (rev1 [1.2] rev2
↪ [1.1] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/GoodStyle (rev1 [1.6] rev2 [1.5] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/InterWikis (rev1 [1.3] rev2 [1.2] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/InterwikiPlugin (rev1 [1.6] rev2 [1.5] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/ManagingTopics (rev1 [1.17] rev2 [1.16]
↪)
```

... continues on next page ...

... continued from previous page ...

```
http://10.0.1.101/twiki/bin/rdiff/TWiki/ManagingWebs (rev1 [1.23] rev2 [1.22] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/PeterThoeny (rev1 [1.4] rev2 [1.3] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/SiteMap (rev1 [1.2] rev2 [1.1] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/StartingPoints (rev1 [1.3] rev2 [1.2] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiAccessControl (rev1 [1.27] rev2 [1.
↪26] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiAdminCookBook (rev1 [1.2] rev2 [1.1
↪] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiFAQ (rev1 [1.12] rev2 [1.11] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiForms (rev1 [1.16] rev2 [1.15] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiFuncModule (rev1 [1.3] rev2 [1.2] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiGlossary (rev1 [1.2] rev2 [1.1] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiHistory (rev1 [1.10] rev2 [1.9] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiInstallationGuide (rev1 [1.53] rev2
↪ [1.52] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiMetaData (rev1 [1.11] rev2 [1.10] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiPlugins (rev1 [1.21] rev2 [1.20] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiPreferences (rev1 [1.47] rev2 [1.46
↪] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiRegistration (rev1 [1.8] rev2 [1.7]
↪ )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiSite (rev1 [1.21] rev2 [1.20] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiSiteTools (rev1 [1.7] rev2 [1.6] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiSkins (rev1 [1.11] rev2 [1.10] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiSystemRequirements (rev1 [1.28] rev
↪2 [1.27] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiTemplates (rev1 [1.18] rev2 [1.17]
↪)
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiTopics (rev1 [1.12] rev2 [1.11] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiTutorial (rev1 [1.12] rev2 [1.11] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiUpgradeGuide (rev1 [1.3] rev2 [1.2]
↪ )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiUserAuthentication (rev1 [1.15] rev
↪2 [1.14] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TWikiVariables (rev1 [1.62] rev2 [1.61]
↪)
http://10.0.1.101/twiki/bin/rdiff/TWiki/TextFormattingFAQ (rev1 [1.14] rev2 [1.1
↪3] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/TextFormattingRules (rev1 [1.37] rev2 [1
↪.36] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/WebChanges (rev1 [1.3] rev2 [1.2] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/WebChangesAlert (rev1 [1.13] rev2 [1.12]
↪ )
http://10.0.1.101/twiki/bin/rdiff/TWiki/WebHome (rev1 [1.78] rev2 [1.77] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/WebIndex (rev1 [1.2] rev2 [1.1] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/WebNotify (rev1 [1.5] rev2 [1.4] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/WebPreferences (rev1 [1.17] rev2 [1.16]
```

... continues on next page ...

... continued from previous page ...

```
↪)
http://10.0.1.101/twiki/bin/rdiff/TWiki/WebSearch (rev1 [1.12] rev2 [1.11] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/WebStatistics (rev1 [1.3] rev2 [1.2] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/WelcomeGuest (rev1 [1.20] rev2 [1.19] )
http://10.0.1.101/twiki/bin/rdiff/TWiki/WindowsInstallCookbook (rev1 [1.3] rev2
↪[1.2] )
http://10.0.1.101/twiki/bin/register/Main/WebHome (Twk1Name [] Twk1WikiName [] T
↪wk1LoginName [] Twk1Email [] Twk0Phone [] Twk0Department [] Twk1Location [] To
↪picName [TWikiRegistration] )
http://10.0.1.101/twiki/bin/rename/TWiki/AppendixFileSystem (newweb [TWiki] newt
↪opic [DocsATWikiFileSystem] confirm [on] )
http://10.0.1.101/twiki/bin/rename/TWiki/FileAttachment (attachment [Sample.txt]
↪ )
http://10.0.1.101/twiki/bin/rename/TWiki/ManagingTopics (newweb [TWiki] newtopic
↪ [RenameTopic] confirm [on] )
http://10.0.1.101/twiki/bin/rename/TWiki/TWikiForms (newweb [TWiki] newtopic [TW
↪ikiFormTemplate] confirm [on] )
http://10.0.1.101/twiki/bin/rename/TWiki/TWikiInstallationGuide (newweb [TWiki]
↪newtopic [TWikiInstallationNotes] confirm [on] )
http://10.0.1.101/twiki/bin/rename/TWiki/TWikiSystemRequirements (newweb [TWiki]
↪ newtopic [TWikiImplementationNotes] confirm [on] )
http://10.0.1.101/twiki/bin/rename/TWiki/TWikiTemplates (newweb [TWiki] newtopic
↪ [TWikiTemplateSystem] confirm [on] )
http://10.0.1.101/twiki/bin/rename/TWiki/TWikiTopics (newweb [TWiki] newtopic [T
↪WikiPages] confirm [on] )
http://10.0.1.101/twiki/bin/rename/TWiki/TWikiUserAuthentication (newweb [TWiki]
↪ newtopic [TWikiAuthentication] confirm [on] )
http://10.0.1.101/twiki/bin/rename/TWiki/WebChangesAlert (newweb [TWiki] newtopi
↪c [WebChangesNotify] confirm [on] )
http://10.0.1.101/twiki/bin/search/Know/ (showlock [] search [%5C.*] web [] nose
↪arch [on] scope [topic] reverse [on] regex [on] limit [100] order [modified] n
↪ototal [] bookview [] nosummary [] casesensitive [] )
http://10.0.1.101/twiki/bin/search/Know/SearchResult (search [] scope [text] nos
↪earch [on] reverse [on] regex [on] order [modified] )
http://10.0.1.101/twiki/bin/search/Main/ (showlock [] search [%5C.*] web [] nose
↪arch [on] scope [topic] reverse [on] regex [on] nototal [] limit [100] order [
↪modified] nosummary [] bookview [] ignorecase [on] casesensitive [] )
http://10.0.1.101/twiki/bin/search/Main/SearchResult (search [] scope [text] nos
↪earch [on] reverse [on] regex [on] order [modified] )
http://10.0.1.101/twiki/bin/search/Sandbox/ (showlock [] search [%5C.*] web [] s
↪cope [topic] nosearch [on] reverse [on] regex [on] order [modified] limit [100
↪] nototal [] bookview [] nosummary [] casesensitive [] )
http://10.0.1.101/twiki/bin/search/Sandbox/SearchResult (search [] scope [text]
↪nosearch [on] reverse [on] regex [on] order [modified] )
http://10.0.1.101/twiki/bin/search/TWiki/ (showlock [] search [] web [] nosearch
↪ [on] scope [topic] reverse [on] regex [on] limit [100] order [modified] notot
↪al [] bookview [] nosummary [] casesensitive [] )
```

... continues on next page ...

... continued from previous page ...

```
http://10.0.1.101/twiki/bin/search/TWiki/SearchResult (search [] scope [text] no
↪search [on] reverse [on] regex [on] order [modified] )
http://10.0.1.101/twiki/bin/upload/Main/WebHome (filename [] filepath [] filecom
↪ment [] createlink [] hidefile [] )
http://10.0.1.101/twiki/bin/upload/TWiki/WebHome (filename [] filepath [] fileco
↪mment [] createlink [] hidefile [] )
http://10.0.1.101/twiki/bin/view/Know/WebChanges (topic [] skin [print] rev [1.1
↪] )
http://10.0.1.101/twiki/bin/view/Know/WebHome (topic [] skin [print] rev [1.9] )
http://10.0.1.101/twiki/bin/view/Know/WebPreferences (topic [] skin [print] rev
↪[1.10] )
http://10.0.1.101/twiki/bin/view/Know/WebSearch (topic [] skin [print] rev [1.8]
↪ )
http://10.0.1.101/twiki/bin/view/Main/OfficeLocations (topic [] skin [print] rev
↪ [1.3] )
http://10.0.1.101/twiki/bin/view/Main/PeterThoeny (topic [] skin [print] rev [1.
↪7] )
http://10.0.1.101/twiki/bin/view/Main/TWikiGroups (topic [] skin [print] rev [1.
↪2] )
http://10.0.1.101/twiki/bin/view/Main/TWikiUsers (topic [] skin [print] rev [1.1
↪5] )
http://10.0.1.101/twiki/bin/view/Main/WebChanges (topic [] skin [print] rev [1.1
↪] )
http://10.0.1.101/twiki/bin/view/Main/WebHome (topic [] skin [print] rev [1.19]
↪unlock [on] )
http://10.0.1.101/twiki/bin/view/Main/WebIndex (topic [] skin [print] rev [1.1]
↪)
http://10.0.1.101/twiki/bin/view/Main/WebNotify (topic [] skin [print] rev [1.6]
↪ )
http://10.0.1.101/twiki/bin/view/Main/WebPreferences (topic [] skin [print] rev
↪[1.12] )
http://10.0.1.101/twiki/bin/view/Main/WebSearch (topic [] skin [print] rev [1.7]
↪ )
http://10.0.1.101/twiki/bin/view/Main/WebStatistics (topic [] skin [print] rev [
↪1.3] )
http://10.0.1.101/twiki/bin/view/Main/WebTopicList (topic [] skin [print] )
http://10.0.1.101/twiki/bin/view/Sandbox/WebChanges (topic [] skin [print] rev [
↪1.1] )
http://10.0.1.101/twiki/bin/view/Sandbox/WebHome (topic [] skin [print] rev [1.6
↪] )
http://10.0.1.101/twiki/bin/view/Sandbox/WebPreferences (topic [] skin [print] r
↪ev [1.9] )
http://10.0.1.101/twiki/bin/view/Sandbox/WebSearch (topic [] skin [print] rev [1
↪.5] )
http://10.0.1.101/twiki/bin/view/TWiki/AppendixFileSystem (topic [] skin [print]
↪ rev [1.11] )
http://10.0.1.101/twiki/bin/view/TWiki/DefaultPlugin (topic [] skin [print] rev
```

... continues on next page ...

... continued from previous page ...

```
↪[1.4] )
http://10.0.1.101/twiki/bin/view/TWiki/FileAttachment (topic [] skin [print] rev
↪ [1.9] )
http://10.0.1.101/twiki/bin/view/TWiki/FormattedSearch (topic [] skin [print] re
↪v [1.8] )
http://10.0.1.101/twiki/bin/view/TWiki/GnuGeneralPublicLicense (topic [] skin [p
↪rint] rev [1.1] )
http://10.0.1.101/twiki/bin/view/TWiki/GoodStyle (topic [] skin [print] rev [1.5
↪] )
http://10.0.1.101/twiki/bin/view/TWiki/InstalledPlugins (topic [] skin [print] )
http://10.0.1.101/twiki/bin/view/TWiki/InstantEnhancements (topic [] skin [print
↪] )
http://10.0.1.101/twiki/bin/view/TWiki/InterWikis (topic [] skin [print] rev [1.
↪2] )
http://10.0.1.101/twiki/bin/view/TWiki/InterwikiPlugin (topic [] skin [print] re
↪v [1.5] )
http://10.0.1.101/twiki/bin/view/TWiki/ManagingTopics (topic [] skin [print] rev
↪ [1.16] )
http://10.0.1.101/twiki/bin/view/TWiki/ManagingWebs (topic [] skin [print] rev [
↪1.22] )
http://10.0.1.101/twiki/bin/view/TWiki/PeterThoeny (topic [] skin [print] rev [1
↪.3] )
http://10.0.1.101/twiki/bin/view/TWiki/SiteMap (topic [] skin [print] rev [1.1]
↪)
http://10.0.1.101/twiki/bin/view/TWiki/StartingPoints (topic [] skin [print] rev
↪ [1.2] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiAccessControl (topic [] skin [print]
↪ rev [1.26] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiAdminCookBook (topic [] skin [print]
↪ rev [1.1] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiDocumentation (topic [] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiFAQ (topic [] skin [print] rev [1.11
↪] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiForms (topic [] skin [print] rev [1.
↪15] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiFuncModule (topic [] skin [print] re
↪v [1.2] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiGlossary (topic [] skin [print] rev
↪[1.1] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiHistory (topic [] skin [print] rev [
↪1.9] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiInstallationGuide (topic [] skin [pr
↪int] rev [1.52] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiMetaData (topic [] skin [print] rev
↪[1.10] raw [debug] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiPlugins (topic [] skin [print] rev [
↪1.20] )
```

... continues on next page ...

... continued from previous page ...

```
http://10.0.1.101/twiki/bin/view/TWiki/TWikiPreferences (topic [] skin [print] r
↪ev [1.46] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiRegistration (topic [] skin [print]
↪rev [1.7] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiShorthand (topic [] skin [print] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiSite (topic [] skin [print] rev [1.2
↪0] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiSiteTools (topic [] skin [print] rev
↪ [1.6] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiSkins (topic [] skin [print] rev [1.
↪10] sel [] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiSystemRequirements (topic [] skin [p
↪rint] rev [1.27] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiTemplates (topic [] skin [print] rev
↪ [1.17] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiTopics (topic [] skin [print] rev [1
↪.11] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiTutorial (topic [] skin [print] rev
↪[1.11] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiUpgradeGuide (topic [] skin [print]
↪rev [1.2] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiUserAuthentication (topic [] skin [p
↪rint] rev [1.14] )
http://10.0.1.101/twiki/bin/view/TWiki/TWikiVariables (topic [] skin [print] rev
↪ [1.61] )
http://10.0.1.101/twiki/bin/view/TWiki/TextFormattingFAQ (topic [] skin [print]
↪rev [1.13] )
http://10.0.1.101/twiki/bin/view/TWiki/TextFormattingRules (topic [] skin [print
↪] rev [1.36] )
http://10.0.1.101/twiki/bin/view/TWiki/WebChanges (topic [] skin [print] rev [1.
↪2] )
http://10.0.1.101/twiki/bin/view/TWiki/WebChangesAlert (topic [] skin [print] re
↪v [1.12] )
http://10.0.1.101/twiki/bin/view/TWiki/WebHome (topic [] skin [print] rev [1.77]
↪ unlock [on] )
http://10.0.1.101/twiki/bin/view/TWiki/WebIndex (topic [] skin [print] rev [1.1]
↪ )
http://10.0.1.101/twiki/bin/view/TWiki/WebNotify (topic [] skin [print] rev [1.4
↪] )
http://10.0.1.101/twiki/bin/view/TWiki/WebPreferences (topic [] skin [print] rev
↪ [1.16] )
http://10.0.1.101/twiki/bin/view/TWiki/WebSearch (topic [] skin [print] rev [1.1
↪1] )
http://10.0.1.101/twiki/bin/view/TWiki/WebStatistics (topic [] skin [print] rev
↪[1.2] )
http://10.0.1.101/twiki/bin/view/TWiki/WebTopicList (topic [] skin [print] )
http://10.0.1.101/twiki/bin/view/TWiki/WelcomeGuest (topic [] skin [print] rev [
```

... continues on next page ...

... continued from previous page ...

```
↪1.19] )
http://10.0.1.101/twiki/bin/view/TWiki/WindowsInstallCookbook (topic [] skin [pr
↪int] rev [1.2] )
http://10.0.1.101/twiki/bin/viewfile/TWiki/FileAttachment (filename [Sample.txt]
↪ rev [] )
http://10.0.1.101/twiki/bin/viewfile/TWiki/TWiki/FileAttachment (rev [] filename
↪ [Sample.txt] )
http://10.0.1.101/view/TWiki/TWikiHistory (rev [1.9] )
```

Log Method
Details:CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 4576 $

Log (CVSS: 0.0)
NVT: HTTP OS Identification

Summary
This script performs HTTP based OS detection from the HTTP banner or default tes
↪t pages.

OID of test routine: 1.3.6.1.4.1.25623.1.0.111067

Vulnerability Detection Result
Detected OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Concluded from HTTP Server banner : Server: Apache/2.2.8 (Ubuntu) DAV/2

Log Method
Details:HTTP OS Identification
OID:1.3.6.1.4.1.25623.1.0.111067
Version used: $Revision: 4479 $

Log (CVSS: 0.0)
NVT: PHP Version Detection (Remote)

Summary
Detection of installed version of PHP.
  This script sends HTTP GET request and try to get the version from the
  response, and sets the result in KB.

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.800109

Vulnerability Detection Result

```
Detected PHP
Version: 5.2.4
Location: tcp/80
CPE: cpe:/a:php:php:5.2.4
Concluded from version 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: 4492 $`

Log (CVSS: 0.0)
NVT: TWiki Version Detection

Summary

```
Detection of installed version of
  TWiki.
  This script sends HTTP GET request and try to get the version from the
  response, and sets the result in KB.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.800399

Vulnerability Detection Result

```
Detected TWiki
Version: 01.Feb.2003
Location: /twiki/bin
CPE: cpe:/a:twiki:twiki:01.Feb.2003
Concluded from version identification result:
This site is running TWiki version <strong>01 Feb 2003</strong>
```

Log Method

Details:`TWiki Version Detection`
OID:`1.3.6.1.4.1.25623.1.0.800399`
Version used: `$Revision: 4427 $`

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.900129

Vulnerability Detection Result
Detected phpMyAdmin
Version: 3.1.1
Location: /phpMyAdmin
CPE: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Concluded from version identification result:
Version 3.1.1

Log Method
Details:phpMyAdmin Detection
OID:1.3.6.1.4.1.25623.1.0.900129
Version used: $Revision: 3669 $

Log (CVSS: 0.0)
NVT: Apache Web Server Version Detection

Summary
Detection of installed version of Apache Web Server
The script detects the version of Apache HTTP Server on remote host and sets the KB.

OID of test routine: 1.3.6.1.4.1.25623.1.0.900498

Vulnerability Detection Result
Detected Apache
Version: 2.2.8
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.2.8
Concluded from version identification result:
Server: Apache/2.2.8

... continues on next page ...

... continued from previous page ...

Log Method
Details:Apache Web Server Version Detection
OID:1.3.6.1.4.1.25623.1.0.900498
Version used: $Revision: 4249 $

Log (CVSS: 0.0)
NVT: TikiWiki Version Detection

Summary
Detection of TikiWiki, a open source web application
is a wiki-based CMS (http://tiki.org/tiki-index.php).
The script sends a connection request to the web server and attempts to
extract the version number from the reply.

OID of test routine: 1.3.6.1.4.1.25623.1.0.901001

Vulnerability Detection Result
Detected TikiWiki
Version: 1.9.5
Location: /tikiwiki
CPE: cpe:/a:tikiwiki:tikiwiki:1.9.5
Concluded from version identification result:
version 1.9.5

Log Method
Details:TikiWiki Version Detection
OID:1.3.6.1.4.1.25623.1.0.901001
Version used: $Revision: 2642 $

[return to 10.0.1.101]

2.1.38 Log 445/tcp

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 aut

... continues on next page ...

... continued from previous page ...

```
↪hentication.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102011

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: 4391 $

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 aut
↪hentication.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102011

Vulnerability Detection Result

```
Detected Samba
Version: 3.0.20
Location: 445/tcp
CPE: cpe:/a:samba:samba:3.0.20
Concluded from version identification result:
Samba 3.0.20-Debian
Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.0.20-Debian
```

Log Method

Details:SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: $Revision: 4391 $

Log (CVSS: 0.0)
NVT: SMB log in

Summary
This script attempts to logon into the remote host using
login/password credentials.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10394

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: 4391 $

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.11011

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: 4261 $

[return to 10.0.1.101]

2.1.39 Log 2121/tcp

Log (CVSS: 0.0)
NVT: FTP Banner Detection

Summary
This Plugin detects the FTP Server Banner and the Banner
of the 'HELP' command.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10092

Vulnerability Detection Result
Remote FTP server banner :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.0.1.101]

Log Method
Details:FTP Banner Detection
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: $Revision: 3690 $

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Vulnerability Detection Result
An FTP server is running on this port.
Here is its banner :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.0.1.101]

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 3923 $

Log (CVSS: 0.0)
NVT: FTP OS Identification

Summary
This script performs FTP banner based OS detection.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105355

Vulnerability Detection Result
Detected OS: Debian GNU/Linux
CPE: cpe:/o:debian:debian_linux
Concluded from FTP banner : 220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.0.1.101
↪]

Log Method
Details:FTP OS Identification
OID:1.3.6.1.4.1.25623.1.0.105355
Version used: $Revision: 4411 $

Log (CVSS: 0.0)
NVT: ProFTPD Server Remote Version Detection

Summary
This script detects the installed version of ProFTP Server
and sets the version in KB.

OID of test routine: 1.3.6.1.4.1.25623.1.0.900815

Vulnerability Detection Result
Detected ProFTPD
Version: 1.3.1
Location: 2121/tcp
CPE: cpe:/a:proftpd:proftpd:1.3.1
Concluded from version identification result:
ProFTPD 1.3.1

Log Method
Details:ProFTPD Server Remote Version Detection
OID:1.3.6.1.4.1.25623.1.0.900815

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: $Revision: 4260 $

[return to 10.0.1.101]

2.1.40 Log 21/tcp

Log (CVSS: 0.0)
NVT: FTP Banner Detection

Summary

This Plugin detects the FTP Server Banner and the Banner
of the 'HELP' command.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10092

Vulnerability Detection Result

Remote FTP server banner :
220 (vsFTPd 2.3.4)

Log Method

Details:FTP Banner Detection
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: $Revision: 3690 $

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Vulnerability Detection Result

An FTP server is running on this port.

. . . continues on next page . . .

... continued from previous page ...

```
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: 3923 $

Log (CVSS: 0.0)
NVT: FTP OS Identification

Summary
This script performs FTP banner based OS detection.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105355

Vulnerability Detection Result
Detected OS: Linux
CPE: cpe:/o:linux:kernel
Concluded from FTP banner : 220 (vsFTPd 2.3.4)

Log Method
Details:FTP OS Identification
OID:1.3.6.1.4.1.25623.1.0.105355
Version used: $Revision: 4411 $

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.111050

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Detected vsFTPd
Version: 2.3.4
Location: 21/tcp
CPE: cpe:/a:beasts:vsftpd:2.3.4
Concluded from version 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: 4120 $

[return to 10.0.1.101]

2.1.41 Log 1524/tcp

Log (CVSS: 0.0)
NVT: Check for Telnet Server

Summary

```
A telnet Server is running at this host.
   Experts in computer security, such as SANS Institute, and the members of the
   comp.os.linux.security newsgroup recommend that the use of Telnet for remote
   logins should be discontinued under all normal circumstances, for the followi
↪ng
   reasons:
   * Telnet, by default, does not encrypt any data sent over the connection
     (including passwords), and so it is often practical to eavesdrop on the
     communications and use the password later for malicious purposes
 anybody who
     has access to a router, switch, hub or gateway located on the network betwe
↪en
     the two hosts where Telnet is being used can intercept the packets passing
↪by
     and obtain login and password information (and whatever else is typed) with
↪ any
     of several common utilities like tcpdump and Wireshark.
   * Most implementations of Telnet have no authentication that would ensure
     communication is carried out between the two desired hosts and not intercep
↪ted
     in the middle.
   * Commonly used Telnet daemons have several vulnerabilities discovered over
     the years.
```

... continues on next page ...

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.100074

Vulnerability Detection Result
A telnet server seems to be running on this port

Log Method
Details:Check for Telnet Server
OID:1.3.6.1.4.1.25623.1.0.100074
Version used: $Revision: 3467 $

Log (CVSS: 0.0)
NVT: Detect Server type and version via Telnet

Summary
This detects the Telnet 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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10281

Vulnerability Detection Result
Remote telnet banner :
root@metasploitable:/#

Solution
Change the login banner to something generic.

Log Method
Details:Detect Server type and version via Telnet
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: $Revision: 2837 $

[return to 10.0.1.101]

2.1.42 Log 3306/tcp

Log (CVSS: 0.0)
NVT: Check for Telnet Server

Summary

```
A telnet Server is running at this host.
   Experts in computer security, such as SANS Institute, and the members of the
   comp.os.linux.security newsgroup recommend that the use of Telnet for remote
   logins should be discontinued under all normal circumstances, for the followi
↪ng
   reasons:
   * Telnet, by default, does not encrypt any data sent over the connection
     (including passwords), and so it is often practical to eavesdrop on the
     communications and use the password later for malicious purposes
 anybody who
     has access to a router, switch, hub or gateway located on the network betwe
↪en
     the two hosts where Telnet is being used can intercept the packets passing
↪by
     and obtain login and password information (and whatever else is typed) with
↪ any
     of several common utilities like tcpdump and Wireshark.
   * Most implementations of Telnet have no authentication that would ensure
     communication is carried out between the two desired hosts and not intercep
↪ted
     in the middle.
   * Commonly used Telnet daemons have several vulnerabilities discovered over
     the years.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100074

Vulnerability Detection Result

```
A telnet server seems to be running on this port
```

Log Method

Details:`Check for Telnet Server`
OID:`1.3.6.1.4.1.25623.1.0.100074`
Version used: `$Revision: 3467 $`

Log (CVSS: 0.0)
NVT: MySQL/MariaDB Detection

Summary

```
Detection of installed version of
```

. . . continues on next page . . .

... continued from previous page ...

MySQL/MariaDB.
Detect a running MySQL/MariaDB by getting the banner, Extract the version from the banner and store the information in KB

OID of test routine: 1.3.6.1.4.1.25623.1.0.100152

Vulnerability Detection Result

```
Detected MySQL
Version: 5.0.51a-3ubuntu5
Location: 3306/tcp
CPE: cpe:/a:mysql:mysql:5.0.51a
Concluded from version 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: 4483 $

Log (CVSS: 0.0)
NVT: Detect Server type and version via Telnet

Summary

This detects the Telnet 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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10281

Vulnerability Detection Result

```
Remote telnet banner :
>
5.0.51a-3ubuntu5\020ABhd>H.N,\252\b\002~QWB#&5vwpLi
```

Solution

Change the login banner to something generic.

... continues on next page ...

... continued from previous page ...

Log Method
Details:Detect Server type and version via Telnet
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: $Revision: 2837 $

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Vulnerability Detection Result
An unknown service is running on this port.
It is usually reserved for MySQL

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 3923 $

Log (CVSS: 0.0)
NVT: Database Open Access Vulnerability

Summary
The host is running a Database server and is prone to information
  disclosure vulnerability.

OID of test routine: 1.3.6.1.4.1.25623.1.0.902799

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

MySQL can be accessed by remote attackers

Impact

Successful exploitation could allow an attacker to obtain the sensitive information of the database.
Impact Level: Application

Solution

Restrict Database access to remote systems.

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: 4043 $

References

Other:
URL:https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

[return to 10.0.1.101]

2.1.43 Log 5432/tcp

Log (CVSS: 0.0)
NVT: PostgreSQL Detection

Summary

Detection of PostgreSQL, a open source object-relational database system (http://www.postgresql.org).

The script sends a connection request to the server (user:postgres, DB:postgres) and attempts to extract the version number from the reply.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100151

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Detected PostgreSQL
Version: 8.3.1
Location: 5432/tcp
CPE: cpe:/a:postgresql:postgresql:8.3.1
Concluded from version identification result:
8.3.1
```

Log Method

Details:`PostgreSQL Detection`
OID:`1.3.6.1.4.1.25623.1.0.100151`
Version used: `$Revision: 4301 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Summary

`The SSL/TLS certificate on this port is self-signed.`

OID of test routine: 1.3.6.1.4.1.25623.1.0.103140

Vulnerability Detection Result

```
Certificates which are 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: ED093088706603BFD5DC237399B498DA2D4D31C6
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
```

... continues on next page ...

... continued from previous page ...

```
↪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: ED093088706603BFD5DC237399B498DA2D4D31C6
```

Log Method
Details:SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: $Revision: 4631 $

References
Other:
URL:http://en.wikipedia.org/wiki/Self-signed_certificate

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

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

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 3923 $

Log (CVSS: 0.0)
NVT: PostgreSQL TLS Detection

Summary
The remote PostgreSQL Server supports TLS.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105013

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

Log Method
Details:PostgreSQL TLS Detection
OID:1.3.6.1.4.1.25623.1.0.105013
Version used: $Revision: 4328 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Perfect Forward Secrecy Ciphers Missing

Summary
The remote Service is missing support for SSL/TLS Ciphers supporting Perfect For
↪ward Secrecy.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105092

Vulnerability Detection Result
The remote service does not support perfect forward secrecy ciphers.

Log Method
Details:SSL/TLS: Perfect Forward Secrecy Ciphers Missing
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: $Revision: 4614 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Weak and Supported Ciphers

Summary

```
This routine reports all SSL/TLS ciphers offered by a service.
  As the NVT 'SSL/TLS: Check Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623
↪.1.0.900234) might run into a
  timeout the actual reporting of all supported ciphers takes place in this NVT
↪instead. The script preference 'Report timeout'
  allows you to configure if such an timeout is reported.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

Vulnerability Detection Result

```
Note: The 'List SSL Supported Ciphers' preference of 'SSL Cipher Settings' is se
↪t to 'no'. Because of this only 'Medium', 'Weak' and 'Null' Ciphers are curren
↪tly reported.
No 'Medium', 'Weak' and 'Null' Ciphers offered by this service via the SSLv2 pro
↪tocol.
No 'Medium', 'Weak' and 'Null' Ciphers offered by this service via the SSLv3 pro
↪tocol.
No 'Medium', 'Weak' and 'Null' Ciphers offered by this service via the TLSv1.0 p
↪rotocol.
No 'Medium', 'Weak' and 'Null' Ciphers by this service via the TLSv1.1 protocol.
No 'Medium', 'Weak' and 'Null' Ciphers by this service via the TLSv1.2 protocol.
```

Log Method

Details:SSL/TLS: Report Weak and Supported Ciphers
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: $Revision: 4614 $

Log (CVSS: 0.0)
NVT: Database Open Access Vulnerability

Summary

```
The host is running a Database server and is prone to information
  disclosure vulnerability.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902799

. . . continues on next page . . .

... continued from previous page ...

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.
Impact Level: Application

Solution
Restrict Database access to remote systems.

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: 4043 $

References
Other:
URL:https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

[return to 10.0.1.101]

2.1.44 Log 22/tcp

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.100259

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
```

Log Method

Details:SSH Protocol Versions Supported
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: $Revision: 4484 $

Log (CVSS: 0.0)
NVT: SSH Server type and version

Summary

```
 This detects the SSH Server's type and version by connecting to the server
  and processing the buffer received.
  This information gives potential attackers additional information about the sy
↪stem they are attacking.
  Versions and Types should be omitted where possible.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10267

Vulnerability Detection Result

```
Detected SSH server version: SSH-2.0-OpenSSH_5.1p1 Debian-5ubuntu1
Remote SSH supported authentication: password,publickey
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:5.1p1
Concluded from remote connection attempt with credentials:
  Login: VulnScan
  Password: VulnScan
```

Log Method

Details:SSH Server type and version
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: $Revision: 4549 $

... continues on next page ...

. . . continued from previous page . . .

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

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: 3923 $

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote S
↪SH Service

OID of test routine: 1.3.6.1.4.1.25623.1.0.105565

Vulnerability Detection Result
The following options are supported by the remote ssh service:
kex_algorithms:
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-h
↪ellman-group14-sha1,diffie-hellman-group1-sha1
server_host_key_algorithms:
ssh-rsa,ssh-dss
encryption_algorithms_client_to_server:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr

. . . continues on next page . . .

... continued from previous page ...

```
encryption_algorithms_server_to_client:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
mac_algorithms_client_to_server:
hmac-md5,hmac-sha1,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
Details:SSH Protocol Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: $Revision: 2828 $

Log (CVSS: 0.0)
NVT: SSH OS Identification

Summary
This script performs SSH banner based OS detection.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105586

Vulnerability Detection Result
Detected OS: Ubuntu 9.04
Version: 9.04
CPE: cpe:/o:canonical:ubuntu_linux:9.04
Concluded from SSH banner : SSH-2.0-OpenSSH_5.1p1 Debian-5ubuntu1

Log Method
Details:SSH OS Identification
OID:1.3.6.1.4.1.25623.1.0.105586
Version used: $Revision: 4411 $

[return to 10.0.1.101]

2.1.45 Log 53/udp

Log (CVSS: 0.0)
NVT: DNS Server Detection (UDP)

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 o
↪f
  the website's actual IP address.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

Vulnerability Detection Result

```
The remote DNS server banner is:
9.4.2
```

Log Method

Details:`DNS Server Detection (UDP)`
OID:`1.3.6.1.4.1.25623.1.0.100069`
Version used: `$Revision: 4463 $`

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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10028

Vulnerability Detection Result

```
Detected Bind
Version: 9.4.2
Location: 53/udp
CPE: cpe:/a:isc:bind:9.4.2
Concluded from version identification result:
9.4.2
```

Solution

. . . continues on next page . . .

... continued from previous page ...

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 sourc
↪e.

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: 4542 $

[return to 10.0.1.101]

2.1.46 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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10028

Vulnerability Detection Result

Detected Bind
Version: 9.4.2
Location: 53/tcp
CPE: cpe:/a:isc:bind:9.4.2
Concluded from version 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.

... continues on next page ...

... continued from previous page ...

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 sourc
↪e.
```

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: 4542 $`

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 o
↪f
  the website's actual IP address.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.108018

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: 4463 $`

[return to 10.0.1.101]

2.1.47 Log 25/tcp

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10263

Vulnerability Detection Result
Remote SMTP server banner :
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

Solution
Change the login banner to something generic.

Log Method
Details:SMTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10263
Version used: $Revision: 2599 $

Log (CVSS: 0.0)
NVT: SMTP STARTTLS Detection

Summary
Check if the remote Mailserver supports the STARTTLS command.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103118

Vulnerability Detection Result
The remote Mailserver supports the STARTTLS command.

Log Method
Details:SMTP STARTTLS Detection
OID:1.3.6.1.4.1.25623.1.0.103118
Version used: $Revision: 2558 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Summary
The SSL/TLS certificate on this port is self-signed.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103140

Vulnerability Detection Result
```
Certificates which are 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: ED093088706603BFD5DC237399B498DA2D4D31C6
```

Log Method
Details:SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: $Revision: 4631 $

References
```
Other:
  URL:http://en.wikipedia.org/wiki/Self-signed_certificate
```

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

. . . continues on next page . . .

... continued from previous page ...

another port than 80 or 443 and makes this information
available for other check routines.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

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: 3923 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Perfect Forward Secrecy Ciphers Missing

Summary
The remote Service is missing support for SSL/TLS Ciphers supporting Perfect For
↪ward Secrecy.

OID of test routine: 1.3.6.1.4.1.25623.1.0.105092

Vulnerability Detection Result
The remote service does not support perfect forward secrecy ciphers.

Log Method
Details:SSL/TLS: Perfect Forward Secrecy Ciphers Missing
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: $Revision: 4614 $

Log (CVSS: 0.0)
NVT: SMTP/POP3/IMAP OS Identification

Summary
This script performs SMTP/POP3/IMAP banner based OS detection.

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.111068

Vulnerability Detection Result

```
Detected OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Concluded from SMTP banner : 220 metasploitable.localdomain ESMTP Postfix (Ubunt
↪u)
```

Log Method

Details:SMTP/POP3/IMAP OS Identification
OID:1.3.6.1.4.1.25623.1.0.111068
Version used: $Revision: 4418 $

Log (CVSS: 0.0)
NVT: Postfix SMTP Server Detection

Summary

```
The script checks the SMTP server
  banner for the presence of Postfix.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.111086

Vulnerability Detection Result

```
Detected Postfix
Version: unknown
Location: 25/tcp
CPE: cpe:/a:postfix:postfix
Concluded from version identification result:
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

Log Method

Details:Postfix SMTP Server Detection
OID:1.3.6.1.4.1.25623.1.0.111086
Version used: $Revision: 2598 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Weak and Supported Ciphers

Summary

```
This routine reports all SSL/TLS ciphers offered by a service.
  As the NVT 'SSL/TLS: Check Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623
↪.1.0.900234) might run into a
  timeout the actual reporting of all supported ciphers takes place in this NVT
↪instead. The script preference 'Report timeout'
  allows you to configure if such an timeout is reported.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

Vulnerability Detection Result

```
Note: The 'List SSL Supported Ciphers' preference of 'SSL Cipher Settings' is se
↪t to 'no'. Because of this only 'Medium', 'Weak' and 'Null' Ciphers are curren
↪tly reported.
'Medium', 'Weak' and 'Null' Ciphers offered by this service via the SSLv2 protoc
↪ol:
SSL2_DES_192_EDE3_CBC_WITH_MD5
SSL2_DES_64_CBC_WITH_MD5
SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5
SSL2_RC2_CBC_128_CBC_WITH_MD5
SSL2_RC4_128_EXPORT40_WITH_MD5
SSL2_RC4_128_WITH_MD5
'Medium', 'Weak' and 'Null' Ciphers offered by this service via the SSLv3 protoc
↪ol:
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_MD5
No 'Medium', 'Weak' and 'Null' Ciphers offered by this service via the TLSv1.0 p
↪rotocol.
No 'Medium', 'Weak' and 'Null' Ciphers by this service via the TLSv1.1 protocol.
No 'Medium', 'Weak' and 'Null' Ciphers by this service via the TLSv1.2 protocol.
```

Log Method

Details:SSL/TLS: Report Weak and Supported Ciphers
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: $Revision: 4614 $

[return to 10.0.1.101]

2.1.48 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about
CPE identities (http://cpe.mitre.org/) of operating systems, services and
applications detected during the scan.

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

Vulnerability Detection Result
10.0.1.101|cpe:/a:apache:http_server:2.2.8
10.0.1.101|cpe:/a:beasts:vsftpd:2.3.4
10.0.1.101|cpe:/a:isc:bind:9.4.2
10.0.1.101|cpe:/a:mysql:mysql:5.0.51a
10.0.1.101|cpe:/a:openbsd:openssh:5.1p1
10.0.1.101|cpe:/a:php:php:5.2.4
10.0.1.101|cpe:/a:phpmyadmin:phpmyadmin:3.1.1
10.0.1.101|cpe:/a:postfix:postfix
10.0.1.101|cpe:/a:postgresql:postgresql:8.3.1
10.0.1.101|cpe:/a:proftpd:proftpd:1.3.1
10.0.1.101|cpe:/a:samba:samba:3.0.20
10.0.1.101|cpe:/a:tikiwiki:tikiwiki:1.9.5
10.0.1.101|cpe:/a:twiki:twiki:01.Feb.2003
10.0.1.101|cpe:/a:x.org:x11:11.0
10.0.1.101|cpe:/o:canonical:ubuntu_linux:9.04

Log Method
Details:CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 4482 $

[return to 10.0.1.101]

2.1.49 Log 6667/tcp

Log (CVSS: 0.0)
NVT: Check for Telnet Server

Summary
A telnet Server is running at this host.
Experts in computer security, such as SANS Institute, and the members of the
comp.os.linux.security newsgroup recommend that the use of Telnet for remote

... continues on next page ...

... continued from previous page ...

```
   logins should be discontinued under all normal circumstances, for the followi
↪ng
   reasons:
   * Telnet, by default, does not encrypt any data sent over the connection
     (including passwords), and so it is often practical to eavesdrop on the
     communications and use the password later for malicious purposes
 anybody who
     has access to a router, switch, hub or gateway located on the network betwe
↪en
     the two hosts where Telnet is being used can intercept the packets passing
↪by
     and obtain login and password information (and whatever else is typed) with
↪ any
     of several common utilities like tcpdump and Wireshark.
   * Most implementations of Telnet have no authentication that would ensure
     communication is carried out between the two desired hosts and not intercep
↪ted
     in the middle.
   * Commonly used Telnet daemons have several vulnerabilities discovered over
     the years.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100074

Vulnerability Detection Result

```
A telnet server seems to be running on this port
```

Log Method

Details:`Check for Telnet Server`
OID:`1.3.6.1.4.1.25623.1.0.100074`
Version used: `$Revision: 3467 $`

Log (CVSS: 0.0)
NVT: Detect Server type and version via Telnet

Summary

```
This detects the Telnet 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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10281

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Remote telnet banner :
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using y
↪our IP address instead
```

Solution

```
Change the login banner to something generic.
```

Log Method

Details:`Detect Server type and version via Telnet`
OID:`1.3.6.1.4.1.25623.1.0.10281`
Version used: `$Revision: 2837 $`

[return to 10.0.1.101]

2.1.50 Log 5900/tcp

Log (CVSS: 0.0)
NVT: VNC Server and Protocol Version Detection

Summary

```
The remote host is running a remote display software (VNC)
  Description :
  The remote server is running VNC, a software which permits a
  console to be displayed remotely.
  This allows authenticated users of the remote host to take its
  control remotely.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10342

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
```

... continues on next page ...

... continued from previous page ...

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: 4297 $

Log (CVSS: 0.0)
NVT: VNC security types

Summary
This script checks the remote VNC protocol version
and the available 'security types'.

OID of test routine: 1.3.6.1.4.1.25623.1.0.19288

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: 4469 $

[return to 10.0.1.101]

2.1.51 Log 512/tcp

Log (CVSS: 0.0)
NVT: Check for Telnet Server

Summary
A telnet Server is running at this host.
Experts in computer security, such as SANS Institute, and the members of the
comp.os.linux.security newsgroup recommend that the use of Telnet for remote
logins should be discontinued under all normal circumstances, for the followi
↪ng
reasons:
* Telnet, by default, does not encrypt any data sent over the connection
(including passwords), and so it is often practical to eavesdrop on the

... continues on next page ...

... continued from previous page ...

```
     communications and use the password later for malicious purposes
 anybody who
     has access to a router, switch, hub or gateway located on the network betwe
↪en
     the two hosts where Telnet is being used can intercept the packets passing
↪by
     and obtain login and password information (and whatever else is typed) with
↪ any
     of several common utilities like tcpdump and Wireshark.
   * Most implementations of Telnet have no authentication that would ensure
     communication is carried out between the two desired hosts and not intercep
↪ted
     in the middle.
   * Commonly used Telnet daemons have several vulnerabilities discovered over
     the years.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100074

Vulnerability Detection Result

```
A telnet server seems to be running on this port
```

Log Method

Details:`Check for Telnet Server`
OID:`1.3.6.1.4.1.25623.1.0.100074`
Version used: `$Revision: 3467 $`

Log (CVSS: 0.0)
NVT: Detect Server type and version via Telnet

Summary

```
This detects the Telnet 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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10281

Vulnerability Detection Result

```
Remote telnet banner :
```

... continues on next page ...

... continued from previous page ...

\001Where are you?

Solution
Change the login banner to something generic.

Log Method
Details:Detect Server type and version via Telnet
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: $Revision: 2837 $

[return to 10.0.1.101]

2.1.52 Log 23/tcp

Log (CVSS: 0.0)
NVT: Detect Server type and version via Telnet

Summary
This detects the Telnet 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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10281

Vulnerability Detection Result
Remote telnet banner :

```
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
```

Solution

... continues on next page ...

... continued from previous page ...

Change the login banner to something generic.

Log Method
Details:Detect Server type and version via Telnet
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: $Revision: 2837 $

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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

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
Version used: $Revision: 3923 $

[return to 10.0.1.101]

2.1.53 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.11011

... continues on next page ...

... continued from previous page ...

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: 4261 $

[return to 10.0.1.101]

2.1.54 Log 137/udp

Log (CVSS: 0.0)
NVT: Using NetBIOS to retrieve information from a Windows host

Summary
The NetBIOS port is open (UDP:137). A remote attacker may use this to gain access to sensitive information such as computer name, workgroup/domain name, currently logged on user name, etc.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10150

Vulnerability Detection Result
```
The following 7 NetBIOS names have been gathered :
 METASPLOITABLE  = This is the computer name registered for workstation services
↪ by a WINS client.
 METASPLOITABLE  = This is the current logged in user registered for this workst
↪ation.
 METASPLOITABLE  = Computer name
   __MSBROWSE__
 WORKGROUP       = Workgroup / Domain name
 WORKGROUP
 WORKGROUP       = Workgroup / Domain name (part of the Browser elections)
. This SMB server seems to be a SAMBA server (this is not a security
risk, this is for your information). This can be told because this server
claims to have a null MAC address
If you do not want to allow everyone to find the NetBios name
of your computer, you should filter incoming traffic to this port.
```

... continues on next page ...

... continued from previous page ...

Solution
Block those ports from outside communication

Log Method
Details:Using NetBIOS to retrieve information from a Windows host
OID:1.3.6.1.4.1.25623.1.0.10150
Version used: $Revision: 3998 $

[return to 10.0.1.101]

2.1.55 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.

OID of test routine: 1.3.6.1.4.1.25623.1.0.11111

Vulnerability Detection Result
```
These are the registered RPC programs:\
\
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 #100005 version 1 'mountd' (mount showmount) on port 35861/TCP
RPC program #100005 version 2 'mountd' (mount showmount) on port 35861/TCP
RPC program #100005 version 3 'mountd' (mount showmount) on port 35861/TCP
RPC program #100024 version 1 'status' on port 37063/TCP
RPC program #100021 version 1 'nlockmgr' on port 53686/TCP
RPC program #100021 version 3 'nlockmgr' on port 53686/TCP
RPC program #100021 version 4 'nlockmgr' on port 53686/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
```

... continues on next page ...

... continued from previous page ...

```
RPC program #100024 version 1 'status' on port 34950/UDP
RPC program #100005 version 1 'mountd' (mount showmount) on port 35580/UDP
RPC program #100005 version 2 'mountd' (mount showmount) on port 35580/UDP
RPC program #100005 version 3 'mountd' (mount showmount) on port 35580/UDP
RPC program #100021 version 1 'nlockmgr' on port 36501/UDP
RPC program #100021 version 3 'nlockmgr' on port 36501/UDP
RPC program #100021 version 4 'nlockmgr' on port 36501/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: 2888 $`

[return to 10.0.1.101]

2.1.56 Log 1099/tcp

Log (CVSS: 0.0)
NVT: RMI-Registry Detection

Summary
`This Script detects the RMI-Registry Service`

OID of test routine: 1.3.6.1.4.1.25623.1.0.105839

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: 4034 $`

[return to 10.0.1.101]