Scan Report

September 25, 2019

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "UTC", which is abbreviated "UTC". The task was "Immediate scan of IP 172.16.108.248". The scan started at Thu Feb 9 20:57:28 2017 UTC and ended at Thu Feb 9 21:07:48 2017 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview **2**

1.1 Host Authentications 2

2 Results per Host **2**

2.1 172.16.108.248 2

2.1.1 High general/tcp 3

2.1.2 High 8787/tcp 4

2.1.3 High 80/tcp 5

2.1.4 High 6000/tcp 12

2.1.5 High 512/tcp 13

2.1.6 High 1524/tcp 14

2.1.7 High 1099/tcp 14

2.1.8 High 3632/tcp 15

2.1.9 High 5432/tcp 16

2.1.10 High 3306/tcp 18

2.1.11 High 22/tcp 18

2.1.12 High 6200/tcp 19

2.1.13 High 21/tcp 20

2.1.14 Medium 80/tcp 21

2.1.15 Medium 5432/tcp 36

2.1.16 Medium 3306/tcp 49

2.1.17 Medium 22/tcp 50

2.1.18 Medium 21/tcp . . . 51
2.1.19 Medium 25/tcp . . . 52
2.1.20 Medium 445/tcp . . . 61
2.1.21 Low general/tcp . . . 62
2.1.22 Low 5432/tcp . . . 63
2.1.23 Low 22/tcp . . . 65
2.1.24 Log general/tcp . . . 66
2.1.25 Log 8787/tcp . . . 69
2.1.26 Log 80/tcp . . . 69
2.1.27 Log 1524/tcp . . . 77
2.1.28 Log 1099/tcp . . . 79
2.1.29 Log 5432/tcp . . . 79
2.1.30 Log 3306/tcp . . . 85
2.1.31 Log 22/tcp . . . 87
2.1.32 Log 21/tcp . . . 89
2.1.33 Log 25/tcp . . . 90
2.1.34 Log 445/tcp . . . 98
2.1.35 Log general/icmp . . . 101
2.1.36 Log general/SMBClient . . . 102
2.1.37 Log general/CPE-T . . . 102
2.1.38 Log 8009/tcp . . . 103
2.1.39 Log 6667/tcp . . . 103
2.1.40 Log 5900/tcp . . . 104
2.1.41 Log 53/tcp . . . 105
2.1.42 Log 514/tcp . . . 106
2.1.43 Log 513/tcp . . . 107
2.1.44 Log 23/tcp . . . 107
2.1.45 Log 2121/tcp . . . 108
2.1.46 Log 139/tcp . . . 109
2.1.47 Log 111/tcp . . . 110

1 Result Overview

Host	High	Medium	Low	Log	False Positive
172.16.108.248	22	43	4	76	0
Total: 1	22	43	4	76	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 145 results selected by the filtering described above. Before filtering there were 323 results.

1.1 Host Authentications

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

2 Results per Host

2.1 172.16.108.248

Host scan start Thu Feb 9 20:57:38 2017 UTC
Host scan end Thu Feb 9 21:07:48 2017 UTC

Service (Port)	Threat Level
general/tcp	High
8787/tcp	High
80/tcp	High
6000/tcp	High
512/tcp	High
1524/tcp	High
1099/tcp	High
3632/tcp	High
5432/tcp	High
3306/tcp	High
22/tcp	High
6200/tcp	High
21/tcp	High
80/tcp	Medium

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
5432/tcp	Medium
3306/tcp	Medium
22/tcp	Medium
21/tcp	Medium
25/tcp	Medium
445/tcp	Medium
general/tcp	Low
5432/tcp	Low
22/tcp	Low
general/tcp	Log
8787/tcp	Log
80/tcp	Log
1524/tcp	Log
1099/tcp	Log
5432/tcp	Log
3306/tcp	Log
22/tcp	Log
21/tcp	Log
25/tcp	Log
445/tcp	Log
general/icmp	Log
general/SMBClient	Log
general/CPE-T	Log
8009/tcp	Log
6667/tcp	Log
5900/tcp	Log
53/tcp	Log
514/tcp	Log
513/tcp	Log
23/tcp	Log
2121/tcp	Log
139/tcp	Log
111/tcp	Log

2.1.1 High general/tcp

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

Summary
OS End Of Life Detection
The Operating System on the remote host has reached the end of life and should not be used anymore

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The Operating System (cpe:/o:canonical:ubuntu_linux:8.04) on the remote host has
↪ reached the end of life at 09 May 2013
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 172.16.108.248]

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.

Vulnerability Detection Result

```
The service is running in $SAFE >= 1 mode. However it is still possible to run a
↪rbitrary syscall commands on the remote host. Sending an invalid syscall the s
↪ervice returned the following response:
Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in `syscall'"0/usr/lib/
↪ruby/1.8/drb/drb.rb:1555:in `send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in `__se
↪nd__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in `perform_without_block'"3/usr/lib/
↪ruby/1.8/drb/drb.rb:1515:in `perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in `m
↪ain_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in `loop'"5/usr/lib/ruby/1.8/drb/
↪drb.rb:1585:in `main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in `start'"5/usr
↪/lib/ruby/1.8/drb/drb.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:143
↪0:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in `start'"//usr/lib/ruby/1.8/dr
↪b/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize'"//us
↪r/lib/ruby/1.8/drb/drb.rb:1627:in `new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
↪`start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
↪plemented
```

Impact

Solution

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

... continues on next page ...

... continued from previous page ...

- Implementing taint on untrusted input

- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

Vulnerability Detection Method

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 172.16.108.248]

2.1.3 High 80/tcp

High (CVSS: 10.0)
NVT: TWiki XSS and Command Execution Vulnerabilities

Product detection result

cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary

The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Vulnerability Detection Result

Installed version: 01.Feb.2003
Fixed version: 4.2.4

Impact

Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.
Impact Level: Application

Solution

Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Upgrade to version 4.2.4 or later, http://twiki.org/cgi-bin/view/Codev/TWikiRelease04x02x04

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight
The flaws are due to, - conduct cross-site scripting attack. - eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details:`TWiki XSS and Command Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: `$Revision: 4227 $`

Product Detection Result
Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
`CVE: CVE-2008-5304, CVE-2008-5305`
`BID:32668, 32669`
`Other:`
`URL:http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304`
`URL:http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305`

High (CVSS: 7.5)
NVT: phpMyAdmin Code Injection and XSS Vulnerability

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary
phpMyAdmin is prone to a remote PHP code-injection vulnerability and to a cross-site scripting vulnerability.
An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system other attacks are also possible.
Versions prior to phpMyAdmin 2.11.9.5 and 3.1.3.1 are vulnerable.

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

... continues on next page ...

... continued from previous page ...

Solution
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:`phpMyAdmin Code Injection and XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100077
Version used: `$Revision: 5016 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
```
CVE: CVE-2009-1151
BID:34236, 34251
Other:
  URL:http://www.securityfocus.com/bid/34236
   URL:http://www.securityfocus.com/bid/34251
```

High (CVSS: 7.5)
NVT: phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities

Product detection result
```
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

Summary
phpMyAdmin is prone to multiple input-validation vulnerabilities, including an HTTP response-splitting vulnerability and a local file-include vulnerability.
These issues can be leveraged to view or execute arbitrary local scripts, or misrepresent how web content is served, cached, or interpreted. This could aid in various attacks that try to entice client users into a false sense of trust. Other attacks are also possible.
Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.

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

Solution
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:`phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100078

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 5016 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
BID:34253
Other:
URL:http://www.securityfocus.com/bid/34253

High (CVSS: 7.5)
NVT: phpMyAdmin Configuration File PHP Code Injection Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
According to its version number, the remote version of phpMyAdmin is prone to a remote PHP code-injection vulnerability.
An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system other attacks are also possible.
phpMyAdmin 3.x versions prior to 3.1.3.2 are vulnerable.

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

Solution
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:phpMyAdmin Configuration File PHP Code Injection Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100144
Version used: $Revision: 5016 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

... continues on next page ...

... continued from previous page ...

CVE: CVE-2009-1285
BID:34526
Other:
URL:http://www.securityfocus.com/bid/34526

High (CVSS: 7.5)
NVT: Tiki Wiki CMS Groupware ¡ 4.2 Multiple Unspecified Vulnerabilities

Product detection result
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)

Summary
Tiki Wiki CMS Groupware is prone to multiple unspecified vulnerabilities, including:
- An unspecified SQL-injection vulnerability - An unspecified authentication-bypass vulnerability
- An unspecified vulnerability

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 4.2

Impact
Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible.

Solution
Solution type: VendorFix
The vendor has released an advisory and fixes. Please see the references for details.

Affected Software/OS
Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.

Vulnerability Detection Method
Details:Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100537
Version used: $Revision: 5144 $

Product Detection Result
Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection
OID: 1.3.6.1.4.1.25623.1.0.901001)

... continues on next page ...

... continued from previous page ...

References

```
CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136
BID:38608
Other:
  URL:http://www.securityfocus.com/bid/38608
   URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=247
↪34
   URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=250
↪46
   URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254
↪24
   URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254
↪35
   URL:http://info.tikiwiki.org/article86-Tiki-Announces-3-5-and-4-2-Releases
   URL:http://info.tikiwiki.org/tiki-index.php?page=homepage
```

High (CVSS: 7.5)
NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result
`Vulnerable url: http://172.16.108.248/cgi-bin/php`

Impact
Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer other attacks are also possible.

Solution
Solution type: VendorFix
PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.

Vulnerability Insight

An example of the -s command, allowing an attacker to view the source code of index.php is below:
http://localhost/index.php?-s

Vulnerability Detection Method
Details:`PHP-CGI-based setups vulnerability when parsing query string parameters from ph.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: `$Revision: 3062 $`

... continues on next page ...

... continued from previous page ...

References

```
CVE: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335
BID:53388
Other:
  URL:http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-r
↪isks-Update-1567532.html
   URL:http://www.kb.cert.org/vuls/id/520827
   URL:http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
   URL:https://bugs.php.net/bug.php?id=61910
   URL:http://www.php.net/manual/en/security.cgi-bin.php
   URL:http://www.securityfocus.com/bid/53388
```

High (CVSS: 7.5)
NVT: Test HTTP dangerous methods

Summary

Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files.

Vulnerability Detection Result

```
We could upload the following files via the PUT method at this web server:
http://172.16.108.248/dav/puttest1580722056.html
We could delete the following files via the DELETE method at this web server:
http://172.16.108.248/dav/puttest1580722056.html
```

Impact

- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.
- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Solution

Solution type: Mitigation
Use access restrictions to these dangerous HTTP methods or disable them completely.

Vulnerability Detection Method

Details:`Test HTTP dangerous methods`
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: `$Revision: 4295 $`

References

```
BID:12141
Other:
  OWASP:OWASP-CM-001
```

High (CVSS: 7.5)
NVT: phpinfo() output accessible

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

Vulnerability Detection Result
```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information to the remote attacker:
http://172.16.108.248/phpinfo.php
http://172.16.108.248/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 address of the host, the web server version, the system version(unix / linux), and the root directory of the web server.

Solution
Solution type: Workaround
Delete them or restrict access to the listened files.

Vulnerability Detection Method
Details:`phpinfo() output accessible`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `$Revision: 3669 $`

[return to 172.16.108.248]

2.1.4 High 6000/tcp

High (CVSS: 0.0)
NVT: X Server Detection

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

... continues on next page ...

... continued from previous page ...

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
```

Log Method

Details:`X Server Detection`
OID:1.3.6.1.4.1.25623.1.0.10407
Version used: `$Revision: 2837 $`

[return to 172.16.108.248]

2.1.5 High 512/tcp

High (CVSS: 10.0)
NVT: Check for rexecd Service

Summary

Rexecd Service is running at this Host. Rexecd (Remote Process Execution) has the same kind of functionality that rsh has : you can execute shell commands on a remote computer.
The main difference is that rexecd authenticate by reading the username and password *unencrypted* from the socket.

Vulnerability Detection Result

```
The rexecd Service is not allowing connections from this host.
```

Solution

Solution type: Mitigation
Disable rexec Service.

Vulnerability Detection Method

Details:`Check for rexecd Service`
OID:1.3.6.1.4.1.25623.1.0.100111
Version used: `$Revision: 4378 $`

References

```
Other:
  URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0618
```

[return to 172.16.108.248]

2.1.6 High 1524/tcp

High (CVSS: 10.0) NVT: Possible Backdoor: Ingreslock
Summary A backdoor is installed on the remote host
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 isystem.
Solution **Solution type:** Workaround
Vulnerability Detection Method Details:`Possible Backdoor: Ingreslock` OID:1.3.6.1.4.1.25623.1.0.103549 Version used: `$Revision: 4718 $`

[return to 172.16.108.248]

2.1.7 High 1099/tcp

High (CVSS: 10.0) NVT: Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability
Summary Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution **Solution type:** Workaround Disable class-loading.
Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software. An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.

Vulnerability Detection Method
Check if the target tries to load a Java class via a remote HTTP URL.
Details:`Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerabil.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.140051
Version used: `$Revision: 4422 $`

References
`Other:`
`URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=23665`

[return to 172.16.108.248]

2.1.8 High 3632/tcp

High (CVSS: 9.3)
NVT: DistCC Remote Code Execution Vulnerability

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

Vulnerability Detection Result
`It was possible to execute the "id" command.`
`Result: uid=1(daemon) gid=1(daemon)`

Solution
Solution type: VendorFix
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: 5120 $`

References
`CVE: CVE-2004-2687`
`Other:`
`URL:http://distcc.samba.org/security.html`

... continues on next page ...

... continued from previous page ...

URL:http://archives.neohapsis.com/archives/bugtraq/2005-03/0183.html

High (CVSS: 8.5)
NVT: DistCC Detection

Summary
DistCC is a program to distribute builds of C, C++, Objective C or Objective C++ code across several machines on a network. DistCC should always generate the same results as a local build, is simple to install and use, and is often two or more times faster than a local compile.

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

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

Solution
Solution type: Mitigation
For more information about DistCC's security see: http://distcc.samba.org/security.html

Vulnerability Detection Method
Details:DistCC Detection
OID:1.3.6.1.4.1.25623.1.0.12638
Version used: $Revision: 5120 $

[return to 172.16.108.248]

2.1.9 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.

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

... continues on next page ...

. . . continued from previous page . . .

Version used: `$Revision: 3911 $`

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

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

Summary
PostgreSQL is prone to multiple security vulnerabilities.

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

Impact
Attackers can exploit these issues to bypass certain security restrictions and execute arbitrary Perl or Tcl code.

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

Affected Software/OS
These issues affect versions prior to the following PostgreSQL versions:
8.4.4
8.3.11
8.2.17
8.1.21
8.0.25
7.4.29

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

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
`CVE: CVE-2010-1169, CVE-2010-1170, CVE-2010-1447`

. . . continues on next page . . .

... continued from previous page ...

```
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 172.16.108.248]

2.1.10 High 3306/tcp

High (CVSS: 9.0)
NVT: MySQL / MariaDB weak password

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

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

Solution
Solution type: Mitigation
Change the password as soon as possible.

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

[return to 172.16.108.248]

2.1.11 High 22/tcp

High (CVSS: 7.5)
NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.
As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

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

Solution
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Try to login with a number of known default credentials via the SSH protocol.
Details:SSH Brute Force Logins With Default Credentials Reporting
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: $Revision: 4508 $

[return to 172.16.108.248]

2.1.12 High 6200/tcp

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

Summary
vsftpd is prone to a backdoor vulnerability.

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

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

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

Affected Software/OS
The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method
Details:vsftpd Compromised Source Packages Backdoor Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: $Revision: 5026 $

References
BID:48539
Other:

... continues on next page ...

... continued from previous page ...

```
  URL:http://www.securityfocus.com/bid/48539
   URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↪doored.html
   URL:https://security.appspot.com/vsftpd.html
```

[return to 172.16.108.248]

2.1.13 High 21/tcp

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

Summary
vsftpd is prone to a backdoor vulnerability.

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

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

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

Affected Software/OS
The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method
Details:`vsftpd Compromised Source Packages Backdoor Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: `$Revision: 5026 $`

References

```
BID:48539
Other:
  URL:http://www.securityfocus.com/bid/48539
   URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↪doored.html
   URL:https://security.appspot.com/vsftpd.html
```

[return to 172.16.108.248]

2.1.14 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10

Product detection result
`cpe:/a:twiki:twiki:01.Feb.2003`
`Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)`

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 4.3.2`

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later, For updates refer to http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Affected Software/OS
TWiki version prior to 4.3.2

Vulnerability Insight
Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method
Details:`TWiki Cross-Site Request Forgery Vulnerability - Sep10`
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: `$Revision: 4293 $`

Product Detection Result
Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
`CVE: CVE-2009-4898`

. . . continues on next page . . .

... continued from previous page ...

Other:
URL:http://www.openwall.com/lists/oss-security/2010/08/03/8
URL:http://www.openwall.com/lists/oss-security/2010/08/02/17
URL:http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix

Medium (CVSS: 6.5)
NVT: phpMyAdmin Bookmark Security Bypass Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to a security-bypass vulnerability that affects bookmarks.
Successfully exploiting this issue allows a remote attacker to bypass certain security restrictions and perform unauthorized actions.
Versions prior to phpMyAdmin 3.3.9.2 and 2.11.11.3 are vulnerable.

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

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

Vulnerability Detection Method
Details:phpMyAdmin Bookmark Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103076
Version used: $Revision: 3911 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2011-0986, CVE-2011-0987
BID:46359
Other:
URL:https://www.securityfocus.com/bid/46359
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2011-2.php

Medium (CVSS: 6.0)
NVT: TWiki Cross-Site Request Forgery Vulnerability

Product detection result
`cpe:/a:twiki:twiki:01.Feb.2003`
`Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)`

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery Vulnerability.

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 4.3.1`

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 4.3.1 or later, http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Affected Software/OS
TWiki version prior to 4.3.1

Vulnerability Insight
Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.

Vulnerability Detection Method
Details:`TWiki Cross-Site Request Forgery Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: `$Revision: 4892 $`

Product Detection Result
Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
`CVE: CVE-2009-1339`
`Other:`
`URL:http://secunia.com/advisories/34880`
`URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258`

... continues on next page ...

... continued from previous page ...

URL:http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff-cve-2009-1339.txt

Medium (CVSS: 5.8)
NVT: http TRACE XSS attack

Summary
Debugging functions are enabled on the remote HTTP server.
The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Vulnerability Detection Result

```
Solution:
Add the following lines for each virtual host in your configuration file :
    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]
See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
```

Solution
Disable these methods.

Vulnerability Detection Method
Details:http TRACE XSS attack
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: $Revision: 3362 $

References

```
CVE: CVE-2004-2320, CVE-2003-1567
BID:9506, 9561, 11604
Other:
  URL:http://www.kb.cert.org/vuls/id/867593
```

Medium (CVSS: 5.0)
NVT: /doc directory browsable

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

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerable url: http://172.16.108.248/doc/

Solution
Solution type: Mitigation
Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:
¡Directory /usr/doc¿ AllowOverride None order deny,allow deny from all allow from localhost ¡/Directory¿

Vulnerability Detection Method
Details:/doc directory browsable
OID:1.3.6.1.4.1.25623.1.0.10056
Version used: $Revision: 4288 $

References
CVE: CVE-1999-0678
BID:318

Medium (CVSS: 5.0)
NVT: awiki Multiple Local File Include Vulnerabilities

Summary
awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result
Vulnerable url: http://172.16.108.248/mutillidae/index.php?page=/etc/passwd

Impact
An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host other attacks are also possible.

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

Affected Software/OS
awiki 20100125 is vulnerable other versions may also be affected.

Vulnerability Detection Method
Details:awiki Multiple Local File Include Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.103210
Version used: $Revision: 5147 $

... continues on next page ...

... continued from previous page ...

References
BID:49187
Other:
URL:http://www.securityfocus.com/bid/49187
URL:http://www.kobaonline.com/awiki/

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability

Product detection result
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)

Summary
The host is installed with Tiki Wiki CMS Groupware and is prone to a local file inclusion vulnerability.

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 12.11

Impact
Successful exploitation will allow an user having access to the admin backend to gain access to arbitrary files and to compromise the application.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Tiki Wiki CMS Groupware version 12.11 LTS, 15.4 or later. For updates refer to https://tiki.org

Affected Software/OS
Tiki Wiki CMS Groupware versions:
- below 12.11 LTS
- 13.x, 14.x and 15.x below 15.4

Vulnerability Insight

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check the version is vulnerable or not.
Details:Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.108064
Version used: $Revision: 5144 $

Product Detection Result
Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
CVE: CVE-2016-10143
Other:
URL:http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-released
URL:https://sourceforge.net/p/tikiwiki/code/60308/

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability

Product detection result
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

Summary
The host is installed with Tiki Wiki CMS Groupware and is prone to input sanitation weakness vulnerability.

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 2.2

Impact
Successful exploitation could allow arbitrary code execution in the context of an affected site.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 2.2 or latest http://info.tikiwiki.org/tiki-index.php?page=Get+Tiki
bl

Affected Software/OS
Tiki Wiki CMS Groupware version prior to 2.2 on all running platform

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The vulnerability is due to input validation error in tiki-error.php which fails to sanitise before being returned to the user.

Vulnerability Detection Method
Details:Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800315
Version used: $Revision: 5144 $

Product Detection Result
Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
CVE: CVE-2008-5318, CVE-2008-5319
Other:
URL:http://secunia.com/advisories/32341
URL:http://info.tikiwiki.org/tiki-read_article.php?articleId=41

Medium (CVSS: 7.5)
NVT: phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to SQL-injection and cross-site scripting vulnerabilities because it fails to sufficiently sanitize user- supplied data.
Exploiting these issues could allow an attacker to steal cookie- based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.
Versions prior to phpMyAdmin 2.11.9.6 and 3.2.2.1 are affected.

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

Solution
Vendor updates are available. Please see the references for details.

Vulnerability Detection Method
Details:phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100307
Version used: $Revision: 5016 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2009-3696, CVE-2009-3697
BID:36658
Other:
URL:http://www.securityfocus.com/bid/36658
URL:http://www.phpmyadmin.net/
URL:http://freshmeat.net/projects/phpmyadmin/releases/306669
URL:http://freshmeat.net/projects/phpmyadmin/releases/306667

Medium (CVSS: 4.3)
NVT: phpMyAdmin Multiple Cross Site Scripting Vulnerabilities

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.
An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks.
The following versions are vulnerable:
phpMyAdmin 2.11.x prior to 2.11.10.1 phpMyAdmin 3.x prior to 3.3.5.1

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

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

Vulnerability Detection Method
Details:phpMyAdmin Multiple Cross Site Scripting Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100761
Version used: $Revision: 3911 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

CVE: CVE-2010-3056
BID:42584
Other:
URL:https://www.securityfocus.com/bid/42584
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-5.php

Medium (CVSS: 4.3)
NVT: phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability

Product detection result

cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary

phpMyAdmin is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.
Versions prior to phpMyAdmin 3.3.6 are vulnerable other versions may also be affected.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

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

Vulnerability Detection Method

Details:phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100775
Version used: $Revision: 3911 $

Product Detection Result

Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

CVE: CVE-2010-2958
BID:42874

... continues on next page ...

... continued from previous page ...

Other:
URL:https://www.securityfocus.com/bid/42874
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-6.php
URL:http://www.phpmyadmin.git.sourceforge.net/git/gitweb.cgi?p=phpmyadmin/php
↪myadmin;a=commitdiff;h=133a77fac7d31a38703db2099a90c1b49de62e37

Medium (CVSS: 4.3)
NVT: phpMyAdmin Database Search Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.
Versions prior to phpMyAdmin 3.3.8.1 and 2.11.11.1 are vulnerable.

Vulnerability Detection Result
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:phpMyAdmin Database Search Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100939
Version used: $Revision: 3911 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2010-4329
BID:45100
Other:
URL:https://www.securityfocus.com/bid/45100
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-8.php

Medium (CVSS: 4.3)
NVT: phpMyAdmin SQL bookmark XSS Vulnerability

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary
This host is running phpMyAdmin and is prone to Cross Site Scripting vulnerability.

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

Impact
Successful exploitation will let the attacker cause XSS attacks and inject malicious web script or HTML code via a crafted SQL bookmarks.

Solution

revision=12608
*** Note: Ignore the warning if above mentioned patches are applied. *****

Affected Software/OS
phpMyAdmin version 3.0.x to 3.2.0.rc1

Vulnerability Insight
This flaw arises because the input passed into SQL bookmarks is not adequately sanitised before using it in dynamically generated content.

Vulnerability Detection Method
Details:`phpMyAdmin SQL bookmark XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800595
Version used: `$Revision: 4869 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
`CVE: CVE-2009-2284`
`BID:35543`
`Other:`
`URL:http://secunia.com/advisories/35649`
`URL:http://www.phpmyadmin.net/home_page/security/PMASA-2009-5.php`

Medium (CVSS: 4.3)
NVT: phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

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

Impact
Successful exploitation will allow attackers to execute arbitrary web script or HTML in a user's browser session in the context of an affected site. Impact Level: Application

Solution

Affected Software/OS
phpMyAdmin versions 3.x before 3.3.7

Vulnerability Insight
The flaw is caused by an unspecified input validation error when processing spoofed requests sent to setup script, which could be exploited by attackers to cause arbitrary scripting code to be executed on the user's browser session in the security context of an affected site.

Vulnerability Detection Method
Details:`phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801286
Version used: `$Revision: 3166 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
`CVE: CVE-2010-3263`
`Other:`
`URL:http://secunia.com/advisories/41210`
`URL:http://xforce.iss.net/xforce/xfdb/61675`
`URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-7.php`

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

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

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.
Impact Level: Application

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

Affected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight
The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Vulnerability Detection Method
Details:`phpMyAdmin 'error.php' Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: `$Revision: 3166 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
`CVE: CVE-2010-4480`
`Other:`
`URL:http://www.exploit-db.com/exploits/15699/`

... continues on next page ...

... continued from previous page ...

URL:http://www.vupen.com/english/advisories/2010/3133

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary
This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

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

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Apache HTTP Server version 2.2.22 or later, For updates refer to http://httpd.apache.org/

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21

Vulnerability Insight
The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method
Details:Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: $Revision: 3566 $

References
CVE: CVE-2012-0053
BID:51706
Other:
URL:http://secunia.com/advisories/47779
URL:http://www.exploit-db.com/exploits/18442
URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
URL:http://httpd.apache.org/security/vulnerabilities_22.html
URL:http://svn.apache.org/viewvc?view=revision&revision=1235454
URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l

[return to 172.16.108.248]

2.1.15 Medium 5432/tcp

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

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

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

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

Impact
Attackers can exploit these issues to shut down affected servers, perform certain actions with elevated privileges, and bypass authentication mechanisms to perform unauthorized actions. Other attacks may also be possible.

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

Vulnerability Detection Method
Details:PostgreSQL Multiple Security Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100273
Version used: $Revision: 5016 $

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
CVE: CVE-2009-3229, 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

...continues on next page ...

... continued from previous page ...

URL:http://permalink.gmane.org/gmane.comp.security.oss.general/2088

Medium (CVSS: 6.8)
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Summary
OpenSSL is prone to security-bypass vulnerability.

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

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

Solution
Solution type: VendorFix
Updates are available.

Affected Software/OS
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h

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

Vulnerability Detection Method
Send two SSL ChangeCipherSpec request and check the response.
Details:SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105042
Version used: $Revision: 4679 $

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

Product detection result

... continues on next page ...

... continued from previous page ...

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

Summary
PostgreSQL is prone to a security-bypass vulnerability because the application fails to properly validate the domain name in a signed CA certificate, allowing attackers to substitute malicious SSL certificates for trusted ones.
PostgreSQL is also prone to a local privilege-escalation vulnerability.

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

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

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

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

Vulnerability Detection Method
Details:PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnera.
↪..
OID:1.3.6.1.4.1.25623.1.0.100400
Version used: $Revision: 5016 $

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
CVE: CVE-2009-4034, CVE-2009-4136
BID:37334, 37333
Other:
URL:http://www.securityfocus.com/bid/37334
URL:http://www.securityfocus.com/bid/37333
URL:http://www.postgresql.org
URL:http://www.postgresql.org/support/security
URL:http://www.postgresql.org/about/news.1170

Medium (CVSS: 6.5)
NVT: PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability

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

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

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

Impact
Attackers can exploit this issue to execute arbitrary code with elevated privileges or crash the affected application.

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

Affected Software/OS
PostgreSQL version 8.0.x, 8.1.x, 8.3.x is vulnerable other versions may also be affected.

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

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
```
CVE: CVE-2010-0442
BID:37973
Other:
  URL:http://www.postgresql.org/
   URL:http://www.securityfocus.com/bid/37973
   URL:http://xforce.iss.net/xforce/xfdb/55902
   URL:http://intevydis.blogspot.com/2010/01/postgresql-8023-bitsubstr-overflow.
↪html
```

Medium (CVSS: 6.5)
NVT: PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability

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

Summary
PostgreSQL is prone to a buffer-overflow vulnerability because the application fails to perform adequate boundary checks on user-supplied data. The issue affects the 'intarray' module.

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

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

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

Affected Software/OS
The issue affect versions prior to 8.2.20, 8.3.14, 8.4.7, and 9.0.3.

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

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
`CVE: CVE-2010-4015`
`BID:46084`
`Other:`
`URL:https://www.securityfocus.com/bid/46084`
`URL:http://www.postgresql.org/`
`URL:http://www.postgresql.org/about/news.1289`

... continues on next page ...

. . . continued from previous page . . .

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

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

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

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

Impact
Exploiting this issue allows local attackers to gain elevated privileges and execute arbitrary commands with the privileges of the victim.

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

Affected Software/OS
Versions prior to PostgreSQL 9.0.1 are vulnerable.

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

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
CVE: CVE-2010-3433
BID:43747
Other:
URL:https://www.securityfocus.com/bid/43747
URL:http://www.postgresql.org/docs/9.0/static/release-9-0-1.html
URL:http://www.postgresql.org
URL:http://www.postgresql.org/support/security

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

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

Summary
PostgreSQL is prone to an unauthorized-access vulnerability.

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

Impact
Attackers can exploit this issue to reset special parameter settings only a root user should be able to modify. This may aid in further attacks.

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

Affected Software/OS
This issue affects versions prior to the following PostgreSQL versions:
7.4.29
8.0.25
8.1.21
8.2.17
8.3.11
8.4.4

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

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
`CVE: CVE-2010-1975`
`BID:40304`
`Other:`
`URL:http://www.securityfocus.com/bid/40304`
`URL:http://www.postgresql.org/docs/current/static/release-8-4-4.html`

... continues on next page ...

... continued from previous page ...

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

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

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

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

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details:SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: $Revision: 4765 $

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

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

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: $Revision: 4863 $

References
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary
... continues on next page ...

... continued from previous page ...

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.8
↪02067) NVT.
```

Impact

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

Solution

Solution type: Mitigation

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight

The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:
- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)
- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method

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: 4686 $`

References

```
CVE: CVE-2016-0800, CVE-2014-3566
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/
   URL:https://drownattack.com/
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

... continues on next page ...

... continued from previous page ...

Summary
This host is prone to an information disclosure vulnerability.

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

Impact
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
Impact Level: Application

Solution
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes

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

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details:SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: $Revision: 4749 $

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

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

... continues on next page ...

... continued from previous page ...

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

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

Impact
Exploiting this issue may allow attackers to terminate connections to the PostgreSQL server, denying service to legitimate users.

Solution
Solution type: VendorFix
Updates are available. Update to newer Version.

Vulnerability Detection Method
Details:`PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100157
Version used: `$Revision: 5016 $`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
`CVE: CVE-2009-0922`
`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 using a cryptographically weak hashing algorithm.

Vulnerability Detection Result
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
```

... continues on next page ...

... continued from previous page ...

```
Signature Algorithm:  sha1WithRSAEncryption
```

Solution
Solution type: Mitigation
Servers that use SSL/TLS certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL/TLS certificates to avoid these web browser SSL/TLS certificate warnings.

Vulnerability Insight
Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not secure enough for ongoing use. Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when users visit web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

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: 4781 $`

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).

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details:`SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `$Revision: 4739 $`

References
```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 172.16.108.248]

2.1.16 Medium 3306/tcp

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

Product detection result
`cpe:/a:mysql:mysql:5.0.51a`
`Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)`

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

Vulnerability Detection Result
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
Solution type: VendorFix
Upgrade to MySQL version 5.0.88 or 5.1.41 For updates refer to http://dev.mysql.com/downloads

Affected Software/OS
MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 on all running platform.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

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: 4869 $

Product Detection Result
Product: cpe:/a:mysql:mysql:5.0.51a
Method: MySQL/MariaDB Detection
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
CVE: CVE-2009-4019, CVE-2009-4028
Other:
URL:http://bugs.mysql.com/47780
URL:http://bugs.mysql.com/47320
URL:http://marc.info/?l=oss-security&m=125881733826437&w=2
URL:http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html

[return to 172.16.108.248]

2.1.17 Medium 22/tcp

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

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

Vulnerability Detection Result
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

... continues on next page ...

... continued from previous page ...

```
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution
Solution type: Mitigation
Disable the weak encryption algorithms.

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

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

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

[return to 172.16.108.248]

2.1.18 Medium 21/tcp

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

Summary
This FTP Server allows anonymous logins.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
It was possible to login to the remote FTP service with the following anonymous
↪account:
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
Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Vulnerability Detection Method
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: 4987 $

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

[return to 172.16.108.248]

2.1.19 Medium 25/tcp

Medium (CVSS: 6.8)
NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability

Summary
Multiple vendors' implementations of STARTTLS are prone to a vulnerability that lets attackers inject arbitrary commands.

... continues on next page ...

... continued from previous page ...

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

Impact
An attacker can exploit this issue to execute arbitrary commands in the context of the user running the application. Successful exploits can allow attackers to obtain email usernames and passwords.

Solution
Updates are available.

Affected Software/OS
The following vendors are affected:
Ipswitch Kerio Postfix Qmail-TLS Oracle SCO Group spamdyke ISC

Vulnerability Detection Method
Send a special crafted STARTTLS request and check the response.
Details:`Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.103935
Version used: `$Revision: 2780 $`

References
```
CVE: CVE-2011-0411, CVE-2011-1430, CVE-2011-1431, CVE-2011-1432, CVE-2011-1575,
↪CVE-2011-1926, CVE-2011-2165
BID:46767
Other:
  URL:http://www.securityfocus.com/bid/46767
   URL:http://kolab.org/pipermail/kolab-announce/2011/000101.html
   URL:http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424
   URL:http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7
   URL:http://www.kb.cert.org/vuls/id/MAPG-8D9M4P
   URL:http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-
↪notes.txt
   URL:http://www.postfix.org/CVE-2011-0411.html
   URL:http://www.pureftpd.org/project/pure-ftpd/news
   URL:http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNot
↪es_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf
   URL:http://www.spamdyke.org/documentation/Changelog.txt
   URL:http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?inclu
↪de_text=1
   URL:http://www.securityfocus.com/archive/1/516901
   URL:http://support.avaya.com/css/P8/documents/100134676
   URL:http://support.avaya.com/css/P8/documents/100141041
   URL:http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html
   URL:http://inoa.net/qmail-tls/vu555316.patch
```

... continues on next page ...

... continued from previous page ...

URL:http://www.kb.cert.org/vuls/id/555316

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests. VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc. OpenVAS suggests that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Detection Result
'VRFY root' produces the following answer: 252 2.0.0 root

Solution
Solution type: Workaround

Vulnerability Detection Method
Details:Check if Mailserver answer to VRFY and EXPN requests
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: $Revision: 2837 $

References
Other:
URL:http://cr.yp.to/smtp/vrfy.html

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

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

Vulnerability Detection Result
The certificate of the remote service expired on 2010-04-16 14:07:45.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of

... 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 (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details:`SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `$Revision: 4765 $`

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary
It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and S
↪SLv3 protocols and supports one or more ciphers. Those supported ciphers can b
↪e found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.
↪25623.1.0.802067) NVT.
```

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

Solution
Solution type: Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight
The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:
- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)
- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method
Check the used protocols of the services provided by this system.
Details:`SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `$Revision: 4686 $`

References
`CVE: CVE-2016-0800, CVE-2014-3566`
`Other:`
`URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report`
`URL:https://bettercrypto.org/`
`URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/`
`URL:https://drownattack.com/`
`URL:https://www.imperialviolet.org/2014/10/14/poodle.html`

Medium (CVSS: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an information disclosure vulnerability.

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

Impact
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.
Impact Level: Application

Solution
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details:SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ...
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: $Revision: 4749 $

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-exploiting-ssl-30.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

Summary

Vulnerability Detection Result
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

Impact

Impact Level: Application

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later For updates refer to https://www.openssl.org

Affected Software/OS

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

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

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details:SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: $Revision: 4781 $

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

Summary

Vulnerability Detection Result
'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

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

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution
Solution type: VendorFix

- If running OpenSSL updateto version 1.0.2b or 1.0.1n or later, For updates refer to https://www.openssl.org

Affected Software/OS

- OpenSSL version before 1.0.2b and 1.0.1n

Vulnerability Insight

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details:SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)
OID:1.3.6.1.4.1.25623.1.0.805188
Version used: $Revision: 4781 $

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 using a cryptographically weak hashing algorithm.

Vulnerability Detection Result
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX

... continues on next page ...

... continued from previous page ...

Signature Algorithm: sha1WithRSAEncryption

Solution
Solution type: Mitigation
Servers that use SSL/TLS certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL/TLS certificates to avoid these web browser SSL/TLS certificate warnings.

Vulnerability Insight
Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not secure enough for ongoing use. Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when users visit web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

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: 4781 $

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).

Vulnerability Detection Result
Server Temporary Key Size: 512 bits

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details:`SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `$Revision: 4739 $`

References
```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 172.16.108.248]

2.1.20 Medium 445/tcp

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

Product detection result
`cpe:/a:samba:samba:3.0.20`
`Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)`

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

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

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

Solution
Solution type: VendorFix
Updates are available. Please see the referenced vendor advisory.

Affected Software/OS
This issue affects Samba 3.0.0 to 3.0.25rc3.

... 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 execution.
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 $`

Product Detection Result
Product: `cpe:/a:samba:samba:3.0.20`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
`CVE: CVE-2007-2447`
`BID:23972`
`Other:`
`URL:http://www.securityfocus.com/bid/23972`
`URL:https://www.samba.org/samba/security/CVE-2007-2447.html`

[return to 172.16.108.248]

2.1.21 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

Vulnerability Detection Result
```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 162157
Paket 2: 162258
```

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

Solution
Solution type: Mitigation

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

. . . continues on next page . . .

... continued from previous page ...

See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

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

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details:`TCP timestamps`
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 172.16.108.248]

2.1.22 Low 5432/tcp

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

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

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

Vulnerability Detection Result
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
Solution type: VendorFix

... 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. ******

Affected Software/OS
PostgreSQL version 8.4.1 and prior and 8.5 through 8.5alpha2

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 $`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
`CVE: CVE-2010-0733`
`Other:`
`URL:https://bugzilla.redhat.com/show_bug.cgi?id=546621`
`URL:http://www.openwall.com/lists/oss-security/2010/03/16/10`
`URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00310.php`
`URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00289.php`
`URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00287.php`
`URL:http://archives.postgresql.org/pgsql-bugs/2009-10/msg00277.php`

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

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

Summary
PostgreSQL is prone to an information-disclosure vulnerability.

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

... continues on next page ...

... continued from previous page ...

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

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

Affected Software/OS
PostgreSQL 8.3.6 is vulnerable other versions may also be affected.

Vulnerability Detection Method
Details:`PostgreSQL Low Cost Function Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100158
Version used: `$Revision: 5016 $`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

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

[return to 172.16.108.248]

2.1.23 Low 22/tcp

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary
The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result
```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
```

... continues on next page ...

... continued from previous page ...

```
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution
Solution type: Mitigation
Disable the weak MAC algorithms.

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

[return to 172.16.108.248]

2.1.24 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional informations which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to openvas-plugins@wald.intevation.org.

Vulnerability Detection Result

```
Best matching OS:
OS: Ubuntu 8.04
Version: 8.04
CPE: cpe:/o:canonical:ubuntu_linux:8.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Debian GNU/Linux
CPE: cpe:/o:debian:debian_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)
Concluded from FTP banner on port 2121/tcp: 220 ProFTPD 1.3.1 Server (Debian) [:
↪:ffff:172.16.108.248]
OS: Linux
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)
Concluded from FTP banner on port 21/tcp: 220 (vsFTPd 2.3.4)
```

... continues on next page ...

... continued from previous page ...

```
OS: Debian GNU/Linux
CPE: cpe:/o:debian:debian_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp: OS String: Debian GNU/Linux; SM
↪B String: Samba 3.0.20-Debian
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.2.8 (Ubuntu)
↪DAV/2
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identificat
↪ion)
Concluded from SMTP banner on port 25/tcp: 220 metasploitable.localdomain ESMTP
↪Postfix (Ubuntu)
OS: Linux 2.6.9 - 2.6.33
CPE: cpe:/o:linux:linux_kernel:2.6
Found by NVT: 1.3.6.1.4.1.25623.1.0.108021 (Nmap OS Identification (NASL wrapper
↪))
Concluded from Nmap TCP/IP fingerprinting:
OS details: Linux 2.6.9 - 2.6.33
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS: Linux Kernel
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint:
(100% confidence)
Linux Kernel
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to openvas-plugins@wald.intevation.org:
Banner:                  _                  _       _ _        _     _      ____
↪
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

... continues on next page ...

... continued from previous page ...

```
metasploitable login:
Identified from: Telnet banner on port 23/tcp
```

Log Method
Details:OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: $Revision: 5130 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Vulnerability Detection Result

```
The following additional but not resolvable hostnames were detected:
ubuntu804-base.localdomain
```

Log Method
Details:SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: $Revision: 4812 $

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 172.16.108.246 to 172.16.108.248:
172.16.108.246
172.16.108.248
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details:Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662

... continues on next page ...

. . . continued from previous page . . .

Version used: $Revision: 4662 $

[return to 172.16.108.248]

2.1.25 Log 8787/tcp

Log (CVSS: 0.0)
NVT: Service Detection with 'GET' Request

Summary
This plugin performs service detection.

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

Log Method
Details:Service Detection with 'GET' Request
OID:1.3.6.1.4.1.25623.1.0.17975
Version used: $Revision: 4944 $

[return to 172.16.108.248]

2.1.26 Log 80/tcp

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

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

Vulnerability Detection Result
The remote web server type is :
Apache/2.2.8 (Ubuntu) DAV/2
Solution : You can set the directive "ServerTokens Prod" to limit
the information emanating from the server in its response headers.

Solution

Log Method
Details:HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: $Revision: 5134 $

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

Summary
This script uses DIRB to find directories and files on web applications via brute forcing. See the preferences section for configuration options.

Vulnerability Detection Result
`This are the directories/files found with brute force:`
`http://172.16.108.248:80/`

Log Method
Details:`DIRB (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: `$Revision: 4685 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A web server is running on this port`

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 4905 $`

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)

- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use

... continues on next page ...

... continued from previous page ...

If you think any of these are wrong please report to openvas-plugins@wald.intevation.org

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 were used for CGI scanning:
http://172.16.108.248/
http://172.16.108.248/cgi-bin
http://172.16.108.248/dav
http://172.16.108.248/doc
http://172.16.108.248/dvwa
http://172.16.108.248/mutillidae
http://172.16.108.248/phpMyAdmin
http://172.16.108.248/scripts
http://172.16.108.248/test
http://172.16.108.248/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
The following directories were excluded from CGI scanning because of the "Regex
↪pattern to exclude directories from CGI scanning" setting of the NVT "Global v
↪ariable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288):
http://172.16.108.248/icons
http://172.16.108.248/mutillidae/javascript
http://172.16.108.248/mutillidae/javascript/ddsmoothmenu
http://172.16.108.248/mutillidae/styles
http://172.16.108.248/mutillidae/styles/ddsmoothmenu
http://172.16.108.248/phpMyAdmin/themes/original/img
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://172.16.108.248/phpMyAdmin/index.php (pma_password [] token [a9e0b35287356
↪0f058b2f75ba67a4192] pma_username [] convcharset [utf-8] table [] lang [] serv
↪er [1] db [] phpMyAdmin [8438919b58afae35a29938362a1cee6d891a627b] )
http://172.16.108.248/phpMyAdmin/phpmyadmin.css.php (token [a9e0b352873560f058b2
↪f75ba67a4192] convcharset [utf-8] js_frame [right] lang [en-utf-8] nocache [24
↪57687151] )
```

Log Method

Details:CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 4964 $

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

Summary

... continues on next page ...

... continued from previous page ...

This plugin uses nikto(1) to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.

Vulnerability Detection Result

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.16.108.248
+ Target Hostname:    172.16.108.248
+ Target Port:        80
+ Start Time:         2017-02-09 20:59:53 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
↪gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
↪to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apach
↪e 2.0.65 (final release) and 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to e
↪asily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59
↪d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause fal
↪se positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
↪ST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the ph
↪pinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databa
↪ses, and should be protected or limited to authorized hosts.
```

... continues on next page ...

... continued from previous page ...

```
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, i
↪node: 92462, size: 40540, mtime: Tue Dec  9 17:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases,
↪ and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpin
↪fo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: Output fr
↪om the phpinfo() function was found.
+ /phpinfo.php?cx[]=KFmYkaZ9QsT12Jw8akMXtnPYZvOnFTIuHFw8xLqsbdL86Mfbc9jbIYGJbRUJ
↪JHyVFLUYnkmdRNigOMOFOFHiduOvNNHbpLXV1Ge0yub3TCY69Lreo2JcAUa56P3QNlOklPoIxiPiRG
↪rLHSz07O4e64ExsWLgMz3yZCnJLqisHt4Gp0le1vwXz6kzpmz8oSde2enmNV7EGEc60eN1EIxvkCJ3
↪96dCMuD7EnqXN4es9CBtkbSBnyG9RfZk7R1VzY9TEljIXwNHmNIpchdGhEtkDKWxTFoHYZq4tfT7gH
↪rudS7qrOLauqOSwy7H7SQw8bEPunGZewooWHMqdVaai3XKlWHVP437e657zP0cYd4RL7mVsy4gGAxZ
↪7yjdQ4hYUnNs9mcMbyFEzvzQZ2X5zJH8tCYBv0TotWi7lfBVvdXxmlqflTaaxWhPymCIpwn2hrq5MA
↪niQxh8VgxEmak3b6t1jlRJERe2WB3akyg7YlNTajo9KYRL1qaa9VuOUjtlS738w5dP8eFeIAA53yas
↪40F93r4O4l2Sr7bU9uJh1SIUb97LMGGrQFfgZNbAQgKPAi6DbwjxyS0lDnwvYoCs8p7KOFYuLqaG1N
↪i80owqbyRtNpfNP6Df85asv1dw604wQpjT9c6n0eJkr7HLPgdlqIc6OkHEosNXQOJE7mQgjEx8sfBP
↪R5Xih5RFkbbIOgap53suJqno0I0ig1ZDVYtZJZ8jStyFXEgZiYTpENKvrmhPGUB3M5mr6CwsoWLgLp
↪WHv0hwq2176UCChOTEasDGgIDp6uI3GIYhoOTJFYuwLlo8eue55kk9eSL7eC4ZVc6h2lE1Li5pte67
↪vq14s4B7IAEzTO4bbLFYkPh3C6e7VxIyGRUaVbPHMnb8C26ncR3lEV4HaS2mQY2EZgLba3jLxIvJ40
↪srUtURq69ELsSJzkub6XWuaI4y89WQmMCKupXsO1jXehgAHqHN5ndN1j7fqZfmt10tQwOie6rN4PfM
↪4PHB2c0VRDM3cjPlrx6J269Fcho26iTGBnRS3ek17mDj3DcuzGTMje4ERHy5ihucBssXJfWPXmrgJK
↪oGkL3USkIONRMxbVJWTSVd0rlhdDFHaeL4rv8vix8MEu62hZGopNLmDXQeeq2dYdtkyxALIxna1WK5
↪9nCmB4eEWWwznUAwKLzs3JQxI3MY2n0WyxMikGvw9Fjfr3SeBwOJAMaTVFBvjmco6qUUAyJd6iYYF5
↪FLDOMcExANdzKWDlOU7iIKAxCDxB5FL5IEK45kTBCrPxWbQvvoYZdXTJLgDlXtkb03baFawD4NYHPb
↪EvhjzaO5MXBsfEJQvZaFwC8JjYwLjKHFxyJIlVt3wA9Bn0bUYyoJmMrNVZ2tZM3xwrbipus3bxfJji
↪NV2okywgl3DEAmyELpeS6tg8eQbCD21qzffoE5VRlBmSsfo1a3HLkDAgWPjYAN9U38XyB1QKnIneA8
↪4JHPlKDayP4qB2m9pg98yx7V1fY4Z9Tia0p3SQZQnCEsEp7rta5sxiXU6Ube1GkK309tpebVd9wINh
↪OgdpdFckplUdTBmLab5cusiZkzopqsGXl5BO2yn685Wt7vbTVlRXruhmv050WfNFRHLJPlC0nKWrrT
↪mwmEP3PkpDl30jfCdDm6SCKTqwqyy5v8lCmuStqndCNqS4S7wpai6bppZ4r8U5Nqt8PEq1ZMGWQ9NT
↪6bQoYspBX62LuXCwfdBBhmtcEPtCl2jaxiZLH7qfGk260FsbkjcwIEY2xYPDQgu59aNrQC6yXFxxs8
↪ucQ7O10an2E5ZVvICPB1ByFxBrTy2LjnVfejPfBis9Vv423MYX4YTTWCOIhMOcn6tYBNT4PSaWBfsp
↪PLa5eAWSxp8ccyeYmhkcg8lon7ZwLXOlKECzNiSwnuULTvg9McA918rUx67Zc4uvyIvBiiyYtyaOm5
↪htcCAwTODtsBetkJxcPeUdj8VVeRW2k83oCqmGCCzOelaEHTa2jftTXKcBQDTIFH8xrm7zBp3R6B1Y
↪i9Rx7mbRSgrOTQD4oVrrmdYKLiYwknhjqPM32tI1pg9m80aa6u5VZ4wewe27dLjiFJYBWJNNmM3Bua
↪9dTRyrmdIrYUlZSXW5cdO2ajlkTGXq33j1N84d4RDQbY4Y7smT8QdcXroHWYUhzuxIFRguvzyRnmP8
↪3O2Rnmal4hUyXhgBNIhSDbbftHOjDj0bOL7EsrYpcVtHXqbsb9uSVbpi6f4hjm09ZLKyPsKRMqB613
↪0qJ7YEjwBP4VnsQYqTiQTcefNdqVfT5pWJZUiBQ4c50FxLrkVMN90HpO60SBHH7bNGdJT6m9wNv7pH
↪9Em9lsjDWZKFCYJ2Is1fNa41eAVC0KnPOCo3OAVduftNLSf6UMB5GtXNIgxelZNVdqlFjNtr544aTR
↪1tAfszgjjAJNTDoTJspUE6dTEqRS2m2f1hYRCi3kA4gqcX8MtB3fxOkxiCLj0ZxyRlKIUIVjwb19At
↪VwrtQRbnJcmlQ1qBbEKGiBq5d17wS8Nf6KTakKeXLbk8n3Y9fhy2AouziEeIra5SVF2Sj4L3JtCjEq
↪p7zdvN5OqNZ3owvBpRMVRI0gzXMAwyCxTnOSVRl1MntqiMGfPaETjKKfTAsbSC2HXpBCvZKDq39WA6
↪HJhi1btMcduVnNuZHqQvRmL1Ir5GNHgB0RtCVuNbnBgKDegJ30sg9VXAcBEOPIl49qhemzrz7yZfq6
```

... continues on next page ...

... continued from previous page ...

```
↪VgRFSYYLgMGE1jPbdmmW621NKzlyKFc7Fpj5dsirjblPLp5I8iL2NkmGBjBCvT9ndg8yeEVjZXLfdM
↪y2DB4wFDNXd6HCkfjrXmendIc4IeSupaJuPpKeN8uDCPu9IVNzoHf2ETmDQzlXqTV4JWCCEa4KwvDB
↪BRKwC1Hv6RoFFNiAJ3vbAA3W2s5X3wEEteuCiXYlXPwurNmvIvw3V8Am4kgNN7U3dfjovvWZod6N2J
↪aTnBlTWE3BKJBVCtURZEsr3gwN2XjxGd8N5Fyqtd8rxhfWV4xSQAJVQ1De4n3JeVDeAdZxctvLmR87
↪EKuBm6nfC9kSSTJrzaAc9X15A1nENAvUGRNi9YAkBkeCd3kCBSfWFxTNZxEMB89aXawLfe69N34yXu
↪hdhxBag3kxxTkVomve61p0h2GQZxE78gB0dyTzzeho9OJQNvuMJ5UHOawYoiPTR5TQtDF9IzRjgFSi
↪Axin8h0CgSyAeb2OrPAxMs7YQUsyPOBhp6G1RxrI0uLfCaEQd6Z6WrNFk82yXV3tvBrcwDPj39fSEs
↪Z2JZGRPTEpJjvNP0G0TWmVuG4Q0wxCKqekHPIFl1CDbMvUdqHjFl9wVZGKtvnxZQQsbk0ZaAb8FR2U
↪gp8mIT5aEovVSTTk2VXDwuDpkeP2FtDD5QbSA5z9jVaiBemIRMjwE0rDBwl4Pilfmoh5G2j8q74WBj
↪44Xx6RZwp4PGQLMXd0JOqpIXwVEz6po90GCQngPagYSYZR7FI8xOgBt1Gg64MujwD4vglTla03GSEI
↪BSuU11jSIzkbJ1ghtOi9mTkaSBFFSPMZiu6KTp2wvRttLyGCGEXmZLuo0gSxrKWa73hJzQ7uKUXrjL
↪lPfMpDiIep0IM03bQpjkT0DitpWZq1XFoSGGQmOUt9OjENpgzme8xwYWqFhlmcwq8OgqY99MshADTp
↪b9Ta6p0Q6WOP0oFxO7YCyjpFOLyEIJRR1rap4q3ghi5aY7cexPYiLIFb7iyVnKQadXrqkyjNLbmzAa
↪1fdn0v2PlbvIUWDu2fmw2mqUpFJsysRTAUmdwhzpYPMrrjZiGnBbmIExbDACnbYgwzp6WnLxamSUeG
↪zQ3a3ngBFEdQIXsnNFnR6NEF7rdjtYFlFkJ9FsAp8nlrGciKZt6REICe5c3NfVQr0sGOihcpFoAD18
↪nZ7NpUfsFoQBOyO06rhVFbh9esLbYNa36TgFHrkjdyWQB2sDRmtEnYaMZR5iROjZUMDvcekMOUMpTe
↪t1KavxYjTyNlx14oeF43MfpT7ObU7K7EhsJUvYmQfWBXX9zPUvW1KpPIRlUMkeZTfaS9tMJCH9Gntc
↪0Et9DYJZ2CDkGCHLWw6GVZF2YcrORVqDGDE5fpTo2FrblEsLbqkOrpkgpC<script>alert(foo)</
↪script>: Output from the phpinfo() function was found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL d
↪atabases, and should be protected or limited to authorized hosts.
+ 8347 requests: 0 error(s) and 29 item(s) reported on remote host
+ End Time:           2017-02-09 21:00:12 (GMT0) (19 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Log Method
Details:Nikto (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: $Revision: 4685 $

Log (CVSS: 0.0)
NVT: Fingerprint web server with favicon.ico

Summary
The remote web server contains a graphic image that is prone to information disclosure.

Vulnerability Detection Result

```
The following apps/services were identified:
"phpmyadmin (2.11.8.1)" fingerprinted by the file: "http://172.16.108.248/phpMyA
↪dmin/favicon.ico"
```

Impact

... continues on next page ...

... continued from previous page ...

The 'favicon.ico' file found on the remote web server belongs to a popular webserver/application. This may be used to fingerprint the webserver/application.

Solution
Solution type: Mitigation
Remove the 'favicon.ico' file or create a custom one for your site.

Log Method
Details:`Fingerprint web server with favicon.ico`
OID:1.3.6.1.4.1.25623.1.0.20108
Version used: `$Revision: 4988 $`

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

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

Vulnerability Detection Result
```
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: 4724 $`

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.

Vulnerability Detection Result
```
Detected TWiki
Version: 01.Feb.2003
Location: /twiki/bin
CPE: cpe:/a:twiki:twiki:01.Feb.2003
```

... continues on next page ...

... continued from previous page ...

```
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.

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.

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
```

Log Method

... continues on next page ...

. . . continued from previous page . . .

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: Tiki Wiki CMS Groupware Version Detection

Summary
Detection of Tiki Wiki CMS Groupware, a open source web application is a wiki-based CMS. The script sends a connection request to the web server and attempts to extract the version number from the reply.

Vulnerability Detection Result

```
Detected Tiki Wiki CMS Groupware
Version: 1.9.5
Location: /tikiwiki
CPE: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Concluded from version identification result:
version 1.9.5
Concluded from version identification location:
http://172.16.108.248/tikiwiki/README
```

Log Method
Details:Tiki Wiki CMS Groupware Version Detection
OID:1.3.6.1.4.1.25623.1.0.901001
Version used: $Revision: 5144 $

References

```
Other:
  URL:http://tiki.org/
```

[return to 172.16.108.248]

2.1.27 Log 1524/tcp

Log (CVSS: 0.0)
NVT: Check for Telnet Server

Summary
A telnet Server is running at this host.

. . . continues on next page . . .

... continued from previous page ...

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 following 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 between 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 intercepted in the middle.
Commonly used Telnet daemons have several vulnerabilities discovered over the years.

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: 4944 $`

Log (CVSS: 0.0)
NVT: Report Telnet Banner

Summary
This scripts reports the received banner of a Telnet Server.

Vulnerability Detection Result
```
Remote telnet banner :
root@metasploitable:/#
```

Impact
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Solution
Change the login banner to something generic.

Log Method
Details:`Report Telnet Banner`
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: `$Revision: 4771 $`

[return to 172.16.108.248]

2.1.28 Log 1099/tcp

Log (CVSS: 0.0) NVT: RMI-Registry Detection
Summary This Script detects the RMI-Registry Service
Vulnerability Detection Result `The RMI-Registry Service is running at this port`
Log Method Details:`RMI-Registry Detection` OID:1.3.6.1.4.1.25623.1.0.105839 Version used: `$Revision: 4034 $`

[return to 172.16.108.248]

2.1.29 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.

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: 4688 $`

Log (CVSS: 0.0) NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

. . . continues on next page . . .

... continued from previous page ...

Summary
The SSL/TLS certificate on this port is self-signed.

Vulnerability Detection Result
```
The certificate of the remote service is self signed.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Log Method
Details:`SSL/TLS: Certificate - Self-Signed Certificate Detection`
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: `$Revision: 4765 $`

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.

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: 4905 $

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

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

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA

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

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

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

Vulnerability Detection Result
The following certificate details of the remote service were collected.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None

... continues on next page ...

... continued from previous page ...

```
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Log Method
Details:SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: $Revision: 4768 $

Log (CVSS: 0.0)
NVT: PostgreSQL TLS Detection

Summary
The remote PostgreSQL Server supports TLS.

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: 4682 $

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

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Vulnerability Detection Result

```
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.0 protocol:
```

... continues on next page ...

... continued from previous page ...

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Log Method
Details:SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: $Revision: 4771 $

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

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

Vulnerability Detection Result
'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.

Log Method
Details:SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: $Revision: 4739 $

Log (CVSS: 0.0)
NVT: Database Open Access Vulnerability

Summary
The host is running a Database server and is prone to information disclosure vulnerability.

Vulnerability Detection Result
`Postgresql database can be accessed by remote attackers`

Impact
Successful exploitation could allow an attacker to obtain the sensitive information of the database.
Impact Level: Application

Solution
Solution type: Workaround
Restrict Database access to remote systems.

Affected Software/OS
- MySQL/MariaDB
- IBM DB2
- PostgreSQL
- IBM solidDB
- Oracle Database
- Microsoft SQL Server

Vulnerability Insight
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_d
↪ss_v1-2.pdf
```

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

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

Vulnerability Detection Result
`'Medium' cipher suites accepted by this service via the SSLv3 protocol:`
`TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA`

. . . continues on next page . . .

... continued from previous page ...

```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
```

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details:`SSL/TLS: Report Medium Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: `$Revision: 4743 $`

[return to 172.16.108.248]

2.1.30 Log 3306/tcp

Log (CVSS: 0.0)
NVT: MySQL/MariaDB Detection

Summary
Detection of installed version of MySQL/MariaDB.
Detect a running MySQL/MariaDB by getting the banner, extract the version from the banner and store the information in KB.

Vulnerability Detection Result

```
Detected MySQL
Version: 5.0.51a-3ubuntu5
Location: 3306/tcp
CPE: cpe:/a:mysql:mysql:5.0.51a
Concluded from version 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: 5046 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
```
An unknown service is running on this port.
It is usually reserved for MySQL
```

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 4905 $`

Log (CVSS: 0.0)
NVT: Database Open Access Vulnerability

Summary
The host is running a Database server and is prone to information disclosure vulnerability.

Vulnerability Detection Result
```
MySQL can be accessed by remote attackers
```

Impact
Successful exploitation could allow an attacker to obtain the sensitive information of the database.
Impact Level: Application

Solution
Solution type: Workaround
Restrict Database access to remote systems.

Affected Software/OS
- MySQL/MariaDB
- IBM DB2
- PostgreSQL
- IBM solidDB
- Oracle Database
- Microsoft SQL Server

Vulnerability Insight
Do not restricting direct access of databases to the remote systems.

Log Method
Details:`Database Open Access Vulnerability`

. . . continues on next page . . .

... continued from previous page ...

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 172.16.108.248]

2.1.31 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

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 system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result
Detected SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Remote SSH supported authentication: password,publickey
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:4.7p1

... continues on next page ...

... continued from previous page ...

```
Concluded from remote connection attempt with credentials:
  Login: VulnScan
  Password: VulnScan
```

Log Method
Details:SSH Server type and version
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: $Revision: 4947 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
An ssh server is running on this port

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 4905 $

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result

```
The following options are supported by the remote ssh service:
kex_algorithms:
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-h
↪ellman-group14-sha1,diffie-hellman-group1-sha1
server_host_key_algorithms:
ssh-rsa,ssh-dss
encryption_algorithms_client_to_server:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
encryption_algorithms_server_to_client:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
mac_algorithms_client_to_server:
```

... continues on next page ...

... continued from previous page ...

```
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 $`

[return to 172.16.108.248]

2.1.32 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.

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: 4780 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result

```
An FTP server is running on this port.
Here is its banner :
```

... continues on next page ...

... continued from previous page ...

```
220 (vsFTPd 2.3.4)
```

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 4905 $`

Log (CVSS: 0.0)
NVT: vsFTPd FTP Server Detection

Summary
The script is grabbing the banner of a FTP server and attempts to identify a vsFTPd FTP Server and its version from the reply.

Vulnerability Detection Result

```
Detected vsFTPd
Version: 2.3.4
Location: 21/tcp
CPE: cpe:/a:beasts:vsftpd:2.3.4
Concluded from version 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: 4777 $`

[return to 172.16.108.248]

2.1.33 Log 25/tcp

Log (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

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

Vulnerability Detection Result

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

... continues on next page ...

... continued from previous page ...

'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: $Revision: 4863 $

References
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html
URL:https://bettercrypto.org/

... continues on next page ...

... continued from previous page ...

URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

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

Summary
This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.

Vulnerability Detection Result
Remote SMTP server banner :
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

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.

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: 4683 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Summary
The SSL/TLS certificate on this port is self-signed.

Vulnerability Detection Result
The certificate of the remote service is self signed.
Certificate details:

... continues on next page ...

... continued from previous page ...

```
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Log Method
Details:SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: $Revision: 4765 $

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.

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: 4905 $

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

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

Vulnerability Detection Result
```
'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
```

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

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

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

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Log Method
Details:SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: $Revision: 4768 $

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

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Vulnerability Detection Result

```
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
```

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details:SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: $Revision: 4771 $

Log (CVSS: 0.0)
NVT: Postfix SMTP Server Detection

Summary
The script checks the SMTP server banner for the presence of Postfix.

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 Supported Cipher Suites

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

Vulnerability Detection Result
```
'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
```

. . . continues on next page . . .

... continued from previous page ...

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

Log Method

Details:SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: $Revision: 4739 $

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

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

Vulnerability Detection Result
```
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
```

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details:`SSL/TLS: Report Medium Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: `$Revision: 4743 $`

[return to 172.16.108.248]

2.1.34 Log 445/tcp

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
. . . continues on next page . . .

... continued from previous page ...

It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result

```
Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.0.20-Debian
Detected OS: Debian GNU/Linux
```

Log Method

Details:`SMB NativeLanMan`
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: `$Revision: 5149 $`

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary

It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result

```
Detected Samba
Version: 3.0.20
Location: 445/tcp
CPE: cpe:/a:samba:samba:3.0.20
Concluded from version 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: 5149 $`

Log (CVSS: 0.0)
NVT: SMB log in

Summary

This script attempts to logon into the remote host using login/password credentials.

Vulnerability Detection Result

```
It was possible to log into the remote host using the SMB protocol.
```

Log Method

... continues on next page ...

. . . continued from previous page . . .

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.

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 $

Log (CVSS: 0.0)
NVT: Microsoft SMB Signing Disabled

Summary
Checking for SMB signing is disabled.
The script logs in via smb, checks the SMB Negotiate Protocol response to confirm SMB signing is disabled.

Vulnerability Detection Result
SMB signing is disabled on this host

Log Method
Details:Microsoft SMB Signing Disabled
OID:1.3.6.1.4.1.25623.1.0.802726
Version used: $Revision: 2576 $

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

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Vulnerability Detection Result
Only SMBv1 is enabled on remote target

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method
Details:SMB Remote Version Detection
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: $Revision: 4262 $

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

Summary
The script detects the Windows SMB Accessible Shares and sets the result into KB.

Vulnerability Detection Result
The following shares were found
IPC$

Log Method
Details:Microsoft Windows SMB Accessible Shares
OID:1.3.6.1.4.1.25623.1.0.902425
Version used: $Revision: 3690 $

[return to 172.16.108.248]

2.1.35 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

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

Log Method
Details:ICMP Timestamp Detection
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: $Revision: 3115 $

References
CVE: CVE-1999-0524
Other:

. . . continues on next page . . .

. . . continued from previous page . . .

URL:http://www.ietf.org/rfc/rfc0792.txt

[return to 172.16.108.248]

2.1.36 Log general/SMBClient

Log (CVSS: 0.0)
NVT: SMB Test with 'smbclient'

Summary
This script tests the remote host SMB Functions with the 'smbclient' tool.

Vulnerability Detection Result
OS Version = UNIX
Domain = WORKGROUP
SMB Serverversion = SAMBA 3.0.20-DEBIAN

Log Method
Details:SMB Test with 'smbclient'
OID:1.3.6.1.4.1.25623.1.0.90011
Version used: $Revision: 4917 $

[return to 172.16.108.248]

2.1.37 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.

Vulnerability Detection Result
172.16.108.248|cpe:/a:apache:http_server:2.2.8
172.16.108.248|cpe:/a:beasts:vsftpd:2.3.4
172.16.108.248|cpe:/a:isc:bind:9.4.2
172.16.108.248|cpe:/a:mysql:mysql:5.0.51a
172.16.108.248|cpe:/a:openbsd:openssh:4.7p1
172.16.108.248|cpe:/a:php:php:5.2.4
172.16.108.248|cpe:/a:phpmyadmin:phpmyadmin:3.1.1
172.16.108.248|cpe:/a:postfix:postfix
172.16.108.248|cpe:/a:postgresql:postgresql:8.3.1

. . . continues on next page . . .

... continued from previous page ...

```
172.16.108.248|cpe:/a:proftpd:proftpd:1.3.1
172.16.108.248|cpe:/a:samba:samba:3.0.20
172.16.108.248|cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
172.16.108.248|cpe:/a:twiki:twiki:01.Feb.2003
172.16.108.248|cpe:/a:x.org:x11:11.0
172.16.108.248|cpe:/o:canonical:ubuntu_linux:8.04
```

Log Method
Details:`CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 4482 $`

[return to 172.16.108.248]

2.1.38 Log 8009/tcp

Log (CVSS: 0.0)
NVT: Service Detection with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.
Note: This plugin is started at the end of a scan to register all remaining unknown services.

Vulnerability Detection Result
`Nmap service detection result for this port: ajp13`

Log Method
Details:`Service Detection with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5118 $`

[return to 172.16.108.248]

2.1.39 Log 6667/tcp

Log (CVSS: 0.0)
NVT: IRC daemon identification

Summary
This script determines the version of the IRC daemon.

Vulnerability Detection Result
`Unable to get the version of this service due to the error:`

... continues on next page ...

... continued from previous page ...

```
ERROR :Closing Link: [172.16.108.246] (Throttled: Reconnecting too fast) -Email
↪admin@Metasploitable.LAN for more information.
```

Log Method
Details:`IRC daemon identification`
OID:1.3.6.1.4.1.25623.1.0.11156
Version used: `$Revision: 4778 $`

Log (CVSS: 0.0)
NVT: Service Detection with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.
Note: This plugin is started at the end of a scan to register all remaining unknown services.

Vulnerability Detection Result

```
Nmap service detection result for this port: irc
```

Log Method
Details:`Service Detection with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5118 $`

[return to 172.16.108.248]

2.1.40 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) which permits a console to be displayed remotely.
This allows authenticated users of the remote host to take its control remotely.

Vulnerability Detection Result

```
A VNC server seems to be running on this port.
The version of the VNC protocol is : RFB 003.003
```

Solution
Make sure the use of this software is done in accordance with your corporate security policy, filter incoming traffic to this port.

Log Method

... continues on next page ...

. . . continued from previous page . . .

Details:VNC Server and Protocol Version Detection
OID:1.3.6.1.4.1.25623.1.0.10342
Version used: $Revision: 4944 $

Log (CVSS: 0.0)
NVT: VNC security types

Summary
This script checks the remote VNC protocol version and the available 'security types'.

Vulnerability Detection Result
The remote VNC server chose security type #2 (VNC authentication)

Log Method
Details:VNC security types
OID:1.3.6.1.4.1.25623.1.0.19288
Version used: $Revision: 4469 $

[return to 172.16.108.248]

2.1.41 Log 53/tcp

Log (CVSS: 0.0)
NVT: Determine which version of BIND name daemon is running

Summary
BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code.

Vulnerability Detection Result
Detected Bind
Version: 9.4.2
Location: 53/tcp
CPE: cpe:/a:isc:bind:9.4.2
Concluded from version identification result:
9.4.2

Solution
Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts.

Vulnerability Insight
The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source.

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method
Details:`Determine which version of BIND name daemon is running`
OID:1.3.6.1.4.1.25623.1.0.10028
Version used: `$Revision: 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 of the website's actual IP address.

Vulnerability Detection Result
```
The remote DNS server banner is:
9.4.2
```

Log Method
Details:`DNS Server Detection (TCP)`
OID:1.3.6.1.4.1.25623.1.0.108018
Version used: `$Revision: 4944 $`

[return to 172.16.108.248]

2.1.42 Log 514/tcp

Log (CVSS: 0.0)
NVT: Service Detection with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.
Note: This plugin is started at the end of a scan to register all remaining unknown services.

Vulnerability Detection Result
```
Nmap service detection result for this port: tcpwrapped
```

Log Method
Details:`Service Detection with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5118 $`

[return to 172.16.108.248]

2.1.43 Log 513/tcp

Log (CVSS: 0.0)
NVT: Service Detection with nmap

Summary
This plugin performs service detection by launching nmap's service probe (nmap -sV) against ports that are running unidentified services.
Note: This plugin is started at the end of a scan to register all remaining unknown services.

Vulnerability Detection Result
```
Nmap service detection result for this port: login
This is a guess. A confident identification of the service was not possible.
```

Log Method
Details:`Service Detection with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 5118 $`

[return to 172.16.108.248]

2.1.44 Log 23/tcp

Log (CVSS: 0.0)
NVT: Report Telnet Banner

Summary
This scripts reports the received banner of a Telnet Server.

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
```

...continues on next page ...

... continued from previous page ...

metasploitable login:

Impact
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Solution
Change the login banner to something generic.

Log Method
Details:Report Telnet Banner
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: $Revision: 4771 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A telnet server seems to be running on this port

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 4905 $

[return to 172.16.108.248]

2.1.45 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.

Vulnerability Detection Result
Remote FTP server banner :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.16.108.248]

Log Method

... continues on next page ...

. . . continued from previous page . . .

Details:FTP Banner Detection
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: $Revision: 4780 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
```
An FTP server is running on this port.
Here is its banner :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.16.108.248]
```

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 4905 $

Log (CVSS: 0.0)
NVT: ProFTPD Server Version Detection (Remote)

Summary
This script detects the installed version of ProFTP Server and sets the version in KB.

Vulnerability Detection Result
```
Detected ProFTPD
Version: 1.3.1
Location: 2121/tcp
CPE: cpe:/a:proftpd:proftpd:1.3.1
Concluded from version identification result:
ProFTPD 1.3.1
```

Log Method
Details:ProFTPD Server Version Detection (Remote)
OID:1.3.6.1.4.1.25623.1.0.900815
Version used: $Revision: 4777 $

[return to 172.16.108.248]

2.1.46 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.

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 172.16.108.248]

2.1.47 Log 111/tcp

Log (CVSS: 0.0)
NVT: Obtain list of all port mapper registered programs via RPC

Summary
This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Vulnerability Detection Result
```
These are the registered RPC programs:
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 43760/TCP
RPC program #100005 version 2 'mountd' (mount showmount) on port 43760/TCP
RPC program #100005 version 3 'mountd' (mount showmount) on port 43760/TCP
RPC program #100024 version 1 'status' on port 49846/TCP
RPC program #100021 version 1 'nlockmgr' on port 52503/TCP
RPC program #100021 version 3 'nlockmgr' on port 52503/TCP
RPC program #100021 version 4 'nlockmgr' on port 52503/TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/UDP
RPC program #100021 version 1 'nlockmgr' on port 40509/UDP
RPC program #100021 version 3 'nlockmgr' on port 40509/UDP
RPC program #100021 version 4 'nlockmgr' on port 40509/UDP
RPC program #100005 version 1 'mountd' (mount showmount) on port 41337/UDP
```

... continues on next page ...

... continued from previous page ...

```
RPC program #100005 version 2 'mountd' (mount showmount) on port 41337/UDP
RPC program #100005 version 3 'mountd' (mount showmount) on port 41337/UDP
RPC program #100024 version 1 'status' on port 53649/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: 4827 $`

Log (CVSS: 0.0)
NVT: RPC portmapper (UDP)

Summary
This script performs detection of RPC portmapper on UDP.

Vulnerability Detection Result
`RPC portmapper is running on this port`

Log Method
Details:`RPC portmapper (UDP)`
OID:1.3.6.1.4.1.25623.1.0.900602
Version used: `$Revision: 4805 $`

[return to 172.16.108.248]