Scan Report

October 6, 2015

Summary

This document reports on the results of an automatic security scan. The scan started at Tue Oct 6 14:30:59 2015 UTC and ended at Tue Oct 6 14:48:01 2015 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
172.30.0.30 (METASPLOITABLE)	Severity: High	41	21	12	76	0
Total: 1		41	21	12	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 150 results selected by the filtering described above. Before filtering there were 151 results.

2 Results per Host

2.1 172.30.0.30

Host scan start Tue Oct 6 14:31:14 2015 UTC
Host scan end Tue Oct 6 14:48:01 2015 UTC

Service (Port)	Threat Level
clm_pts (6200/tcp)	High
distcc (3632/tcp)	High
ftp (21/tcp)	High
http (80/tcp)	High
mysql (3306/tcp)	High
nfs (2049/udp)	High
postgresql (5432/tcp)	High
scientia-ssdb (2121/tcp)	High
ssh (22/tcp)	High
x11 (6000/tcp)	High
http (80/tcp)	Medium
mysql (3306/tcp)	Medium
postgresql (5432/tcp)	Medium
ssh (22/tcp)	Medium
exec (512/tcp)	Medium
general/tcp	Medium
netbios-ssn (139/tcp)	Medium
shell (514/tcp)	Medium
smtp (25/tcp)	Medium
ftp (21/tcp)	Low

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
http (80/tcp)	Low
scientia-ssdb (2121/tcp)	Low
general/tcp	Low
domain (53/tcp)	Low
general/SMBClient	Low
telnet (23/tcp)	Low
tftp (69/udp)	Low
vnc (5900/tcp)	Low
distcc (3632/tcp)	Log
ftp (21/tcp)	Log
http (80/tcp)	Log
mysql (3306/tcp)	Log
postgresql (5432/tcp)	Log
scientia-ssdb (2121/tcp)	Log
ssh (22/tcp)	Log
x11 (6000/tcp)	Log
exec (512/tcp)	Log
general/tcp	Log
netbios-ssn (139/tcp)	Log
shell (514/tcp)	Log
smtp (25/tcp)	Log
domain (53/tcp)	Log
telnet (23/tcp)	Log
vnc (5900/tcp)	Log
ajp13 (8009/tcp)	Log
domain (53/udp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log
ingreslock (1524/tcp)	Log
ircd (6667/tcp)	Log
login (513/tcp)	Log
microsoft-ds (445/tcp)	Log
msgsrvr (8787/tcp)	Log
netbios-ns (137/udp)	Log
nfs (2049/tcp)	Log
rmiregistry (1099/tcp)	Log
sunrpc (111/tcp)	Log

2.1.1 High clm_pts (6200/tcp)

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

... continues on next page ...

... continued from previous page ...

Summary:
vsftpd is prone to a backdoor vulnerability.
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
The vsftpd 2.3.4 source package is affected.
Solution:
The repaired package can be downloaded from https://security.appspot.com/vsftpd.html. Please validate the package with its signature.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103185

References

BID:48539
Other:
URL:http://www.securityfocus.com/bid/48539
URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
URL:https://security.appspot.com/vsftpd.html
URL:http://vsftpd.beasts.org/

[return to 172.30.0.30]

2.1.2 High distcc (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.
Solution:
Vendor updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103553

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2004-2687
Other:
URL:http://distcc.samba.org/security.html
URL:http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2687
URL:http://www.osvdb.org/13378
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.
distcc by default trusts its clients completely that in turn could
allow a malicious client to execute arbitrary commands on the server.
For more information about DistCC's security see:
http://distcc.samba.org/security.html

OID of test routine: 1.3.6.1.4.1.25623.1.0.12638

[return to 172.30.0.30]

2.1.3 High ftp (21/tcp)

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

Summary:
vsftpd is prone to a backdoor vulnerability.
Attackers can exploit this issue to execute arbitrary commands in the
context of the application. Successful attacks will compromise the
affected application.
The vsftpd 2.3.4 source package is affected.
Solution:
The repaired package can be downloaded from
https://security.appspot.com/vsftpd.html. Please validate the package
with its signature.

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.103185

References

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

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

```
  Summary:
  This host is running ProFTPD Server and is prone to remote
  SQL Injection vulnerability.
  Vulnerability Insight:
  This flaw occurs because the server performs improper input sanitising,
  - when a %(percent) character is passed in the username, a single quote
    (') gets introduced during variable substitution by mod_sql and this
    eventually allows for an SQL injection during login.
  - when NLS support is enabled, a flaw in variable substition feature in
    mod_sql_mysql and mod_sql_postgres may allow an attacker to bypass
    SQL injection protection mechanisms via invalid, encoded multibyte
    characters.
  Impact:
  Successful exploitation will allow remote attackers to execute arbitrary
  SQL commands, thus gaining access to random user accounts.
  Affected Software/OS:
  ProFTPD Server version 1.3.1 through 1.3.2rc2
  Solution:
  Upgrade to the latest version 1.3.2rc3,
  http://www.proftpd.org/
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900507

References

```
CVE: CVE-2009-0542, CVE-2009-0543
BID:33722
Other:
  URL:http://www.milw0rm.com/exploits/8037
```

... continues on next page ...

... continued from previous page ...

URL:http://www.securityfocus.com/archive/1/archive/1/500833/100/0/threaded
URL:http://www.securityfocus.com/archive/1/archive/1/500851/100/0/threaded

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

Summary:
ProFTPD is prone to a security-bypass vulnerability because the application fails to properly validate the domain name in a signed CA certificate, allowing attackers to substitute malicious SSL certificates for trusted ones.
Successful exploits allows attackers to perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks.
Versions prior to ProFTPD 1.3.2b and 1.3.3 to 1.3.3.rc1 are vulnerable.
Solution:
Updates are available. Please see the references for details.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100316

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

[return to 172.30.0.30]

2.1.4 High http (80/tcp)

High (CVSS: 10.0)
NVT: PHP version smaller than 5.2.7

Summary:
PHP version smaller than 5.2.7 suffers vulnerability.
Solution:
Update PHP to version 5.2.7 or later.

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.110172

References

CVE: CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, ↪CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE ↪-2008-5658
BID:29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948

High (CVSS: 10.0)
NVT: PHP version smaller than 5.2.6

Summary:
PHP version smaller than 5.2.6 suffers vulnerability.
Solution:
Update PHP to version 5.2.6 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110183

References

CVE: CVE-2007-4850, CVE-2007-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, ↪CVE-2008-2051
BID:27413, 28392, 29009

High (CVSS: 9.3)
NVT: PHP version smaller than 5.2.14

Summary:
PHP version smaller than 5.2.14 suffers vulnerability.
Solution:
Update PHP to version 5.2.14 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110171

References

CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, ↪CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE ↪-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3065

... continues on next page ...

... continued from previous page ...

BID:38708, 40948, 41991

High (CVSS: 9.3)
NVT: PHP version smaller than 5.2.5

Summary:
PHP version smaller than 5.2.5 suffers vulnerability.
Solution:
Update PHP to version 5.2.5 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110179

References

CVE: CVE-2007-3996, CVE-2007-4782, CVE-2007-4783, CVE-2007-4784, CVE-2007-4825,
↪CVE-2007-4840, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE
↪-2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2008-2107, CVE-2008-2108, CVE-20
↪08-4107
BID:26403

High (CVSS: 9.3)
NVT: PHP version smaller than 5.3.3

Summary:
PHP version smaller than 5.3.3 suffers vulnerability.
Solution:
Update PHP to version 5.3.3 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110182

References

CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,
↪CVE-2010-1917, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE
↪-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3062, CVE-20
↪10-3063, CVE-2010-3064, CVE-2010-3065
BID:38708, 40461, 40948, 41991

... continues on next page ...

. . . continued from previous page . . .

High (CVSS: 7.5)
NVT: TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities

Product detection result
cpe:/a:tikiwiki:tikiwiki:1.9.5
Detected by TikiWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

Summary:
TikiWiki is prone to multiple unspecified vulnerabilities, including:
- An unspecified SQL-injection vulnerability
- An unspecified authentication-bypass vulnerability
- An unspecified vulnerability
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.
Versions prior to TikiWiki 4.2 are vulnerable.
Solution:
The vendor has released an advisory and fixes. Please see the references for details.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100537

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
↪=24734
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision
↪=25046
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision
↪=25424
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision
↪=25435
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.

. . . continues on next page . . .

... continued from previous page ...

Summary:
When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the
php-cgi receives a processed query string parameter as command line
arguments which allows command-line switches, such as -s, -d or -c to be
passed to the php-cgi binary, which can be exploited to disclose source
code and obtain arbitrary code execution.
An example of the -s command, allowing an attacker to view the source code
of index.php is below:
http://localhost/index.php?-s

OID of test routine: 1.3.6.1.4.1.25623.1.0.103482

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

High (CVSS: 7.5)
NVT: PHP version smaller than 5.2.11

Summary:
PHP version smaller than 5.2.11 suffers vulnerability.
Solution:
Update PHP to version 5.2.11 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110176

References

CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018,
↪CVE-2009-5016
BID:36449, 44889

High (CVSS: 7.5)
NVT: PHP version smaller than 5.3.1

```
Summary:
PHP version smaller than 5.3.1 suffers vulnerability.
Solution:
Update PHP to version 5.3.1 or later.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.110178

References
CVE: CVE-2009-3557, CVE-2009-3559, CVE-2009-4017, CVE-2009-4018, CVE-2010-1128
BID:36554, 36555, 37079, 37138

High (CVSS: 7.5)
NVT: PHP version smaller than 5.2.8

```
Summary:
PHP version smaller than 5.2.8 suffers vulnerability.
Solution:
Update PHP to version 5.2.8 or later.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.110180

References
CVE: CVE-2008-5814, CVE-2008-5844
BID:32673

High (CVSS: 7.5)
NVT: phpinfo.php

```
The following files are calling the function phpinfo() which
disclose potentially sensitive information to the remote attacker :
/phpinfo.php
Solution: Delete them or restrict access to them
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11229

High (CVSS: 6.8)
NVT: PHP version smaller than 5.3.4

```
Summary:
PHP version smaller than 5.3.4 suffers vulnerability.
Solution:
Update PHP to version 5.3.4 or later.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.110181

References

```
CVE: CVE-2006-7243, CVE-2010-2094, CVE-2010-2950, CVE-2010-3436, CVE-2010-3709,
↪CVE-2010-3710, CVE-2010-3870, CVE-2010-4150, CVE-2010-4156, CVE-2010-4409, CVE
↪-2010-4697, CVE-2010-4698, CVE-2010-4699, CVE-2010-4700, CVE-2011-0753, CVE-20
↪11-0754, CVE-2011-0755
BID:40173, 43926, 44605, 44718, 44723, 44951, 44980, 45119, 45335, 45338, 45339,
↪ 45952, 45954, 46056, 46168
```

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

```
 Summary:
 Debugging functions are enabled on the remote HTTP server.
Description :
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.
 Solution:
 Disable these methods.
Plugin output :
Solution:
Add the following lines for each virtual host in your configuration file :
    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11213

. . . continues on next page . . .

... continued from previous page ...

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

[return to 172.30.0.30]

2.1.5 High mysql (3306/tcp)

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

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

Summary:
MySQL is prone to a buffer-overflow vulnerability because if fails to perform adequate boundary checks on user-supplied data.
An attacker can leverage this issue to execute arbitrary code within the context of the vulnerable application. Failed exploit attempts will result in a denial-of-service condition.
This issue affects MySQL 5.x; other versions may also be vulnerable.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100271

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

High (CVSS: 9.0)
NVT: MySQL weak password

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

... continues on next page ...

... continued from previous page ...

Summary:
It was possible to login into the remote MySQL as root using weak credentials.
Solution:
Change the password as soon as possible.
It was possible to login as root with an empty password.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103551

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

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

Summary:
The host is running MySQL and is prone to Multiple Format String
vulnerabilities.
Vulnerability Insight:
The flaws are due to error in the 'dispatch_command' function in sql_parse.cc
in libmysqld/ which can caused via format string specifiers in a database name
in a 'COM_CREATE_DB' or 'COM_DROP_DB' request.
Impact:
Successful exploitation could allow remote authenticated users to cause a Deni
↪al
of Service and possibly have unspecified other attacks.
Impact Level: Application
Affected Software/OS:
MySQL version 4.0.0 to 5.0.83 on all running platform.
Solution:
Upgrade to MySQL version 5.1.36 or later
http://dev.mysql.com/downloads

OID of test routine: 1.3.6.1.4.1.25623.1.0.800842

References
CVE: CVE-2009-2446
BID:35609
Other:

... continues on next page ...

... continued from previous page ...

URL:http://www.osvdb.org/55734
URL:http://secunia.com/advisories/35767
URL:http://xforce.iss.net/xforce/xfdb/51614
URL:http://www.securityfocus.com/archive/1/archive/1/504799/100/0/threaded

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

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

Summary:
MySQL 5.0.51a is prone to an unspecified remote code-execution vulnerability.
Very few technical details are currently available.
An attacker can leverage this issue to execute arbitrary code within the context of the vulnerable application. Failed exploit attempts will result in a denial-of-service condition.
This issue affects MySQL 5.0.51a; other versions may also be vulnerable.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100436

References
CVE: CVE-2009-4484
BID:37640
Other:
URL:http://www.securityfocus.com/bid/37640
URL:http://archives.neohapsis.com/archives/dailydave/2010-q1/0002.html
URL:http://www.mysql.com/
URL:http://intevydis.com/mysql_demo.html

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

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

... continues on next page ...

... continued from previous page ...

```
  Summary:
  The host is running MySQL and is prone to Buffer overflow
  Vulnerability
  Vulnerability Insight:
  The flaw is due to an error in application that allows remote attackers to
  execute arbitrary code via unspecified vectors
  Impact:
  Successful exploitation could allow attackers to execute arbitrary code.
  Impact Level: Application
  Affected Software/OS:
  MySQL Version 5.0.51a On Linux
  Solution:
  No solution or patch is available as of 31st December, 2009. Information
  regarding this issue will be updated once the solution details are available
  For updates refer to http://dev.mysql.com/downloads
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.901093

References

```
CVE: CVE-2009-4484
Other:
  URL:http://intevydis.com/vd-list.shtml
   URL:http://www.intevydis.com/blog/?p=57
```

High (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 Insight:
  The flaws are due to:
  - mysqld does not properly handle errors during execution of certain SELECT
    statements with subqueries, and does not preserve certain null_value flags
    during execution of statements that use the 'GeomFromWKB()' function.
  - An error in 'vio_verify_callback()' function in 'viosslfactories.c', when
    OpenSSL is used, accepts a value of zero for the depth of X.509 certificates
↪.
  Impact:
```

... continues on next page ...

... continued from previous page ...

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
Affected Software/OS:
MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 on all running platform.
Solution:
Upgrade to MySQL version 5.0.88 or 5.1.41
For updates refer to http://dev.mysql.com/downloads

OID of test routine: 1.3.6.1.4.1.25623.1.0.801064

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

High (CVSS: 6.5)
NVT: MySQL Multiple Vulnerabilities

Product detection result

cpe:/a:mysql:mysql:5.0.51a
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

Summary:
The host is running MySQL and is prone to multiple vulnerabilities.
Vulnerability Insight:
The flaws are due to:
- An error in 'my_net_skip_rest()' function in 'sql/net_serv.cc' when handling a large number of packets that exceed the maximum length, which allows remot
↪e
attackers to cause a denial of service (CPU and bandwidth consumption).
- buffer overflow when handling 'COM_FIELD_LIST' command with a long table name, allows remote authenticated users to execute arbitrary code.
- directory traversal vulnerability when handling a '..' (dot dot) in a table name, which allows remote authenticated users to bypass intended table grants to read field definitions of arbitrary tables.
Impact:
Successful exploitation could allow users to cause a denial of service and to execute arbitrary code.

... continues on next page ...

... continued from previous page ...

Impact Level: Application
Affected Software/OS:
MySQL 5.0.x before 5.0.91 and 5.1.x before 5.1.47 on all running platform.
Solution:
Upgrade to MySQL version 5.0.91 or 5.1.47,
For updates refer to http://dev.mysql.com/downloads

OID of test routine: 1.3.6.1.4.1.25623.1.0.801355

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

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

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

Summary:
The host is running MySQL and is prone to Access Restrictions Bypass
Vulnerability
Vulnerability Insight:
The flaw is due to an error in 'sql/sql_table.cc', when the data home director
↪y
contains a symlink to a different filesystem.
Impact:
Successful exploitation could allow users to bypass intended access restrictio
↪ns
by calling CREATE TABLE with DATA DIRECTORY or INDEX DIRECTORY argument refer
↪ring
to a subdirectory.
Impact Level: Application
Affected Software/OS:
MySQL 5.0.x before 5.0.88, 5.1.x before 5.1.41, 6.0 before 6.0.9-alpha
Solution:
Upgrade to MySQL version 5.0.88 or 5.1.41 or 6.0.9-alpha

... continues on next page ...

... continued from previous page ...

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.801065

References

```
CVE: CVE-2008-7247
Other:
  URL:http://lists.mysql.com/commits/59711
   URL:http://bugs.mysql.com/bug.php?id=39277
   URL:http://marc.info/?l=oss-security&amp;m=125908040022018&amp;w=2
```

[return to 172.30.0.30]

2.1.6 High nfs (2049/udp)

High (CVSS: 10.0)
NVT: NFS export

```
Here is the export list of 172.30.0.30 :
/ *
Please check the permissions of this exports.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102014

References

```
CVE: CVE-1999-0554, CVE-1999-0548
```

[return to 172.30.0.30]

2.1.7 High postgresql (5432/tcp)

High (CVSS: 9.0)
NVT: PostgreSQL weak password

Product detection result

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

... continues on next page ...

... continued from previous page ...

```
 Summary:
 It was possible to login into the remote PostgreSQL as user postgres using weak
↪ credentials.
 Solution:
 Change the password as soon as possible.
It was possible to login as user postgres with password "postgres".
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103552

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.
Attackers can exploit these issues to bypass certain security
restrictions and execute arbitrary Perl or Tcl code.
These issues affect versions prior to the following PostgreSQL
versions:
8.4.4
8.3.11
8.2.17
8.1.21
8.0.25
7.4.29
 Solution:
 Updates are available. Please see the references for more information.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100645

References

```
CVE: CVE-2010-1169, CVE-2010-1170, CVE-2010-1447
BID:40215
Other:
  URL:http://www.securityfocus.com/bid/40215
   URL:http://www.postgresql.org/about/news.1203
   URL:http://www.postgresql.org/
```

... continues on next page ...

... continued from previous page ...

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

High (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.
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:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100273

References
CVE: CVE-2009-3229, CVE-2009-3230, CVE-2009-3231
BID:36314
Other:
URL:http://www.securityfocus.com/bid/36314
URL:https://bugzilla.redhat.com/show_bug.cgi?id=522085#c1
URL:http://www.postgresql.org/
URL:http://www.postgresql.org/support/security
URL:http://permalink.gmane.org/gmane.comp.security.oss.general/2088

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

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

Summary:

... continues on next page ...

... continued from previous page ...

PostgreSQL is prone to a security-bypass vulnerability because the application fails to properly validate the domain name in a signed CA certificate, allowing attackers to substitute malicious SSL certificates for trusted ones.
Successfully exploiting this issue allows attackers to perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks.
PostgreSQL is also prone to a local privilege-escalation vulnerability.
Exploiting this issue allows local attackers to gain elevated privileges.
PostgreSQL versions prior to 8.4.2, 8.3.9, 8.2.15, 8.1.19, 8.0.23, and 7.4.27 are vulnerable to this issue.
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100400

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

High (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.
Attackers can exploit this issue to execute arbitrary code with elevated privileges or crash the affected application.
PostgreSQL version 8.0.x, 8.1.x, 8.3.x is vulnerable; other versions may also be
↪ affected.

... continues on next page ...

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.100470

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
```

High (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.
An authenticated attacker can leverage this issue to execute arbitrary
code within the context of the vulnerable application. Failed exploit
attempts will result in a denial-of-service condition.
The issue affect versions prior to 8.2.20, 8.3.14, 8.4.7, and 9.0.3.
 Solution:
 Updates are available. Please see the references for more information.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103054

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
```

High (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.
Exploiting this issue allows local attackers to gain elevated
privileges and execute arbitrary commands with the privileges of
the victim.
Versions prior to PostgreSQL 9.0.1 are vulnerable.
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100843

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

High (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.
Attackers can exploit this issue to reset special parameter
settings only a root user should be able to modify. This may aid in
further attacks.
This issue affects versions prior to the following PostgreSQL
versions:
7.4.29,

... continues on next page ...

... continued from previous page ...

```
8.0.25
8.1.21,
8.2.17
8.3.11
8.4.4
 Solution:
 Updates are available. Please see the references for more information.



OID of test routine: 1.3.6.1.4.1.25623.1.0.100648
```

References

```
CVE: CVE-2010-1975
BID:40304
Other:
  URL:http://www.securityfocus.com/bid/40304
   URL:http://www.postgresql.org/docs/current/static/release-8-4-4.html
   URL:http://www.postgresql.org/docs/current/static/release-8-2-17.html
   URL:http://www.postgresql.org/docs/current/static/release-8-1-21.html
   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
```

[return to 172.30.0.30]

2.1.8 High scientia-ssdb (2121/tcp)

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

```
  Summary:
  This host is running ProFTPD Server and is prone to remote
  SQL Injection vulnerability.
  Vulnerability Insight:
  This flaw occurs because the server performs improper input sanitising,
  - when a %(percent) character is passed in the username, a single quote
    (') gets introduced during variable substitution by mod_sql and this
    eventually allows for an SQL injection during login.
  - when NLS support is enabled, a flaw in variable substition feature in
    mod_sql_mysql and mod_sql_postgres may allow an attacker to bypass
    SQL injection protection mechanisms via invalid, encoded multibyte
    characters.
  Impact:
```

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow remote attackers to execute arbitrary
SQL commands, thus gaining access to random user accounts.
Affected Software/OS:
ProFTPD Server version 1.3.1 through 1.3.2rc2
Solution:
Upgrade to the latest version 1.3.2rc3,
http://www.proftpd.org/

OID of test routine: 1.3.6.1.4.1.25623.1.0.900507

References

CVE: CVE-2009-0542, CVE-2009-0543
BID:33722
Other:
URL:http://www.milw0rm.com/exploits/8037
URL:http://www.securityfocus.com/archive/1/archive/1/500833/100/0/threaded
URL:http://www.securityfocus.com/archive/1/archive/1/500851/100/0/threaded

High (CVSS: 6.8)
NVT: ProFTPD Long Command Handling Security Vulnerability

Summary:
The host is running ProFTPD Server, which is prone to cross-site
request forgery vulnerability.
Vulnerability Insight:
The flaw exists due to the application truncating an overly long FTP command,
and improperly interpreting the remainder string as a new FTP command.
Impact:
This can be exploited to execute arbitrary FTP commands on another
user's session privileges.
Impact Level : Application
Affected Software/OS:
ProFTPD Project versions 1.2.x on Linux
ProFTPD Project versions 1.3.x on Linux
Solution:
Fixed is available in the SVN repository,
http://www.proftpd.org/cvs.html
*****
NOTE : Ignore this warning, if above mentioned fix is applied already.
*****

OID of test routine: 1.3.6.1.4.1.25623.1.0.900133

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2008-4242
BID:31289
Other:
URL:http://secunia.com/advisories/31930/
URL:http://bugs.proftpd.org/show_bug.cgi?id=3115

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

Summary:
ProFTPD is prone to a security-bypass vulnerability because the application fails to properly validate the domain name in a signed CA certificate, allowing attackers to substitute malicious SSL certificates for trusted ones.
Successful exploits allows attackers to perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks.
Versions prior to ProFTPD 1.3.2b and 1.3.3 to 1.3.3.rc1 are vulnerable.
Solution:
Updates are available. Please see the references for details.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100316

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

[return to 172.30.0.30]

2.1.9 High ssh (22/tcp)

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

... continues on next page ...

... continued from previous page ...

```
 Summary:
 It was possible to login into the remote host using default credentials.
 Solution:
 Change the password as soon as possible.
It was possible to login with the following credentials <User>:<Password>
user:user
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103239

[return to 172.30.0.30]

2.1.10 High x11 (6000/tcp)

High (CVSS: 10.0)
NVT: X Server

```
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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10407

References

```
CVE: CVE-1999-0526
```

[return to 172.30.0.30]

2.1.11 Medium http (80/tcp)

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

```
 Summary:
 The /doc directory is browsable.
/doc shows the content of the /usr/doc directory and therefore it shows which pr
```

... continues on next page ...

... continued from previous page ...

```
↪ograms and - important! - the version of the installed programs.
 Solution:
 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>
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10056

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.
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 computer; other attacks are
also possible.
awiki 20100125 is vulnerable; other versions may also be affected.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103210

References

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

Medium (CVSS: 5.0)
NVT: PHP version smaller than 5.2.9

Summary:
PHP version smaller than 5.2.9 suffers vulnerability.
Solution:
Update PHP to version 5.2.9 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110187

References
CVE: CVE-2008-5498, CVE-2009-1271, CVE-2009-1272
BID:33002, 33927

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

Product detection result
cpe:/a:phpmyadmin:phpmyadmin
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 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.
Impact:
Successful exploitation will allow attackers to inject arbitrary
HTML code within the error page and conduct phishing attacks.
Impact Level: Application
Affected Software/OS:
phpMyAdmin version 3.3.8.1 and prior.
Solution:
No solution or patch was made available for at least one year
since disclosure of this vulnerability. Likely none will be provided anymore.
General solution options are to upgrade to a newer release, disable respective
features, remove the product or replace the product by another one.

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.801660

References

```
CVE: CVE-2010-4480
Other:
  URL:http://www.exploit-db.com/exploits/15699/
   URL:http://www.vupen.com/english/advisories/2010/3133
```

Medium (CVSS: 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 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.
  Impact:
  Successful exploitation will allow attackers to obtain sensitive information
  that may aid in further attacks.
  Impact Level: Application
  Affected Software/OS:
  Apache HTTP Server versions 2.2.0 through 2.2.21
  Solution:
  Upgrade to Apache HTTP Server version 2.2.22 or later,
  For updates refer to http://httpd.apache.org/
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902830

References

```
CVE: CVE-2012-0053
BID:51706
Other:
  URL:http://osvdb.org/78556
   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&amp;revision=1235454
   URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l
```

[return to 172.30.0.30]

2.1.12 Medium mysql (3306/tcp)

Medium (CVSS: 6.4)
NVT: MySQL multiple 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:
MySQL is prone to a security-bypass vulnerability and to to a local privilege-escalation vulnerability.
An attacker can exploit the security-bypass issue to bypass certain security restrictions and obtain sensitive information that may lead to further attacks.
Local attackers can exploit the local privilege-escalation issue to gain elevated privileges on the affected computer.
Versions prior to MySQL 5.1.41 are vulnerable.
Solution:
Updates are available. Please see the references for details.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100356

References
BID:37075, 37076
Other:
URL:http://www.securityfocus.com/bid/37076
URL:http://www.securityfocus.com/bid/37075
URL:http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html
URL:http://www.mysql.com/

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

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

Summary:

...continues on next page ...

... continued from previous page ...

According to its version number, the remote version of MySQL is
prone to a security-bypass vulnerability.
An attacker can exploit this issue to gain access to table files created by
other users, bypassing certain security restrictions.
NOTE 1: This issue was also assigned CVE-2008-4097 because
CVE-2008-2079 was incompletely fixed, allowing symlink attacks.
NOTE 2: CVE-2008-4098 was assigned because fixes for the vector
described in CVE-2008-4097 can also be bypassed.
This issue affects versions prior to MySQL 4 (prior to 4.1.24) and
MySQL 5 (prior to 5.0.60).
Solution:
Updates are available. Update to newer Version.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100156

References

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

Medium (CVSS: 4.0)
NVT: Oracle MySQL 'TEMPORARY InnoDB' Tables Denial Of Service Vulnerability

Product detection result

cpe:/a:mysql:mysql:5.0.51a
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

Summary:
MySQL is prone to a denial-of-service vulnerability.
An attacker can exploit these issues to crash the database, denying
access to legitimate users.
This issues affect versions prior to MySQL 5.1.49.
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100763

References

CVE: CVE-2010-3680

... continues on next page ...

... continued from previous page ...

BID:42598
Other:
URL:https://www.securityfocus.com/bid/42598
URL:http://bugs.mysql.com/bug.php?id=54044
URL:http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html
URL:http://www.mysql.com/

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

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

Summary:
MySQL is prone to a denial-of-service vulnerability.
An attacker can exploit this issue to crash the database, denying
access to legitimate users.
This issue affects versions prior to MySQL 5.1.49.
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100785

References
CVE: CVE-2010-3677
BID:42646, 42633, 42643, 42598, 42596, 42638, 42599, 42625
Other:
URL:https://www.securityfocus.com/bid/42646
URL:https://www.securityfocus.com/bid/42633
URL:https://www.securityfocus.com/bid/42643
URL:https://www.securityfocus.com/bid/42598
URL:https://www.securityfocus.com/bid/42596
URL:https://www.securityfocus.com/bid/42638
URL:https://www.securityfocus.com/bid/42599
URL:https://www.securityfocus.com/bid/42625
URL:http://bugs.mysql.com/bug.php?id=54575
URL:http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html
URL:http://www.mysql.com/

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

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

```
Summary:
This host is running MySQL, which is prone to Denial of Service
Vulnerability.
Vulnerability Insight:
Issue is due to error while processing an empty bit string literal via
       a specially crafted SQL statement.
Impact:
Successful exploitation by remote attackers could cause denying
       access to legitimate users.
Impact Level : Application
Affected Software/OS:
MySQL versions prior to 5.0.x - 5.0.66,
                               5.1.x - 5.1.26, and
                               6.0.x - 6.0.5 on all running platform.
Solution:
Update to version 5.0.66 or 5.1.26 or 6.0.6 or later.
http://dev.mysql.com/downloads/
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900221

References
CVE: CVE-2008-3963
BID:31081
Other:
URL:http://secunia.com/advisories/31769/
URL:http://bugs.mysql.com/bug.php?id=35658
URL:http://dev.mysql.com/doc/refman/5.1/en/news-5-1-26.html

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

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

... continues on next page ...

... continued from previous page ...

```
Summary:
The host is running MySQL and is prone to Denial Of Service
vulnerability.
Vulnerability Insight:
The flaw is due to an error when processing the 'ALTER DATABASE' statement and
can be exploited to corrupt the MySQL data directory using the '#mysql50#'
prefix followed by a '.' or '..'.
NOTE: Successful exploitation requires 'ALTER' privileges on a database.
Impact:
Successful exploitation could allow an attacker to cause a Denial of Service.
Impact Level: Application
Affected Software/OS:
MySQL version priot to 5.1.48 on all running platform.
Solution:
Upgrade to MySQL version 5.1.48
For updates refer to http://dev.mysql.com/downloads
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.801380

References

```
CVE: CVE-2010-2008
BID:41198
Other:
  URL:http://secunia.com/advisories/40333
   URL:http://bugs.mysql.com/bug.php?id=53804
   URL:http://securitytracker.com/alerts/2010/Jun/1024160.html
   URL:http://dev.mysql.com/doc/refman/5.1/en/news-5-1-48.html
```

[return to 172.30.0.30]

2.1.13 Medium postgresql (5432/tcp)

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

Product detection result

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

```
Summary:
PostgreSQL is prone to a remote denial-of-service vulnerability.
 Exploiting this issue may allow attackers to terminate connections
```

... continues on next page ...

... continued from previous page ...

```
  to the PostgreSQL server, denying service to legitimate users.
 Solution:
 Updates are available. Update to newer Version.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100157

References

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

Medium (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 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.
  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
  Affected Software/OS:
  PostgreSQL version 8.4.1 and prior and 8.5 through 8.5alpha2
  Solution:
  Apply the patch,
  http://git.postgresql.org/gitweb?p=postgresql.git;a=commitdiff;h=64b057e682365
↪5fb6c5d1f24a28f236b94dd6c54
  ******
  NOTE: Please ignore this warning if the patch is applied.
  ******
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.902139

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
```

Medium (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.
  Local attackers can exploit this issue to obtain sensitive
  information that may lead to further attacks.
  PostgreSQL 8.3.6 is vulnerable; other versions may also be affected.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100158

References

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

[return to 172.30.0.30]

2.1.14 Medium ssh (22/tcp)

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

```
According to its banner, the version of OpenSSH installed on the remote
host is older than 5.7:
 ssh-2.0-openssh_4.7p1 debian-8ubuntu1
 Summary:
 The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7
provides debug messages containing authorized_keys command options, which allows
remote authenticated users to obtain potentially sensitive information by
reading these messages, as demonstrated by the shared user account required by
Gitolite. NOTE: this can cross privilege boundaries because a user account may
intentionally have no shell or filesystem access, and therefore may have no
supported way to read an authorized_keys file in its own home directory.
OpenSSH before 5.7 is affected;
 Solution:
 Updates are available. Please see the references for more information.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103503

References

```
CVE: CVE-2012-0814
BID:51702
Other:
  URL:http://www.securityfocus.com/bid/51702
   URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445
   URL:http://packages.debian.org/squeeze/openssh-server
   URL:https://downloads.avaya.com/css/P8/documents/100161262
```

[return to 172.30.0.30]

2.1.15 Medium exec (512/tcp)

Medium (CVSS: 5.0)
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.
 Solution:
 Disable rexec Service.
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.100111

[return to 172.30.0.30]

2.1.16 Medium general/tcp

Medium (CVSS: 5.0)
NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability

OID of test routine: 1.3.6.1.4.1.25623.1.0.902815

References

```
CVE: CVE-2004-0230
BID:10183
Other:
  URL:http://www.osvdb.org/4030
   URL:http://xforce.iss.net/xforce/xfdb/15886
   URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html
   URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949
   URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950
   URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006
   URL:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx
   URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx
   URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
   URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
```

Medium (CVSS: 2.6)
NVT: TCP timestamps

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 22475
Paket 2: 22575
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

... continues on next page ...

... continued from previous page ...

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

[return to 172.30.0.30]

2.1.17 Medium netbios-ssn (139/tcp)

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

Summary:
Samba is prone to a remote denial-of-service vulnerability.
A remote attacker can exploit this issue to crash the affected
application, denying service to legitimate users.
Samba 3.4.5 and earlier are vulnerable.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100499

References
CVE: CVE-2010-0547
BID:38326
Other:
URL:http://www.securityfocus.com/bid/38326
URL:http://git.samba.org/?p=samba.git;a=commit;h=a065c177dfc8f968775593ba00df
↪fafeebb2e054
URL:http://us1.samba.org/samba/

[return to 172.30.0.30]

2.1.18 Medium shell (514/tcp)

Medium (CVSS: 0.0)
NVT: Check for rsh Service

Summary:
rsh Service is running at this Host.
rsh (remote shell) is a command line computer program which can execute
shell commands as another user, and on another computer across a computer

... continues on next page ...

... continued from previous page ...

network.
Solution:
Disable rsh and use ssh instead.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100080

[return to 172.30.0.30]

2.1.19 Medium smtp (25/tcp)

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

Summary:
The Mailserver on this host answers to VRFY and/or EXPN requests.
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.
Solution:
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
Details:
'VRFY root' produces the following answer: 252 2.0.0 root

OID of test routine: 1.3.6.1.4.1.25623.1.0.100072

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

[return to 172.30.0.30]

2.1.20 Low ftp (21/tcp)

Low (CVSS: 1.9)
NVT: FTP Server type and version

... continues on next page ...

... continued from previous page ...

```
Remote FTP server banner :
220 (vsFTPd 2.3.4)
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10092

[return to 172.30.0.30]

2.1.21 Low http (80/tcp)

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

```
Here is the Nikto report:
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          172.30.0.30
+ Target Hostname:    172.30.0.30
+ Target Port:        80
+ Start Time:         2015-10-06 14:33:12 (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.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.22). Apach
↪e 1.3.42 (final release) and 2.0.64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microso
↪ft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
↪ST
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals
↪potentially sensitive information via certain HTTP requests that contain speci
↪fic QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databa
↪ses, and should be protected or limited to authorized hosts.
+ Cookie phpMyAdmin created without the httponly flag
+ OSVDB-3092: /phpMyAdmin/: phpMyAdmin is for managing MySQL databases, and shou
↪ld be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, inode: 41
```

... continues on next page ...

... continued from previous page ...

```
↪2190, size: 5108, mtime: 0x438c0358aae80
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ 6544 items checked: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2015-10-06 14:33:51 (GMT0) (39 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.14260

[return to 172.30.0.30]

2.1.22 Low scientia-ssdb (2121/tcp)

Low (CVSS: 1.9)
NVT: FTP Server type and version

```
Remote FTP server banner :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.30.0.30]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10092

[return to 172.30.0.30]

2.1.23 Low general/tcp

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

```
ProFTPD version 1.3.1 was detected on the host
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900815

[return to 172.30.0.30]

2.1.24 Low domain (53/tcp)

Low (CVSS: 5.0)
NVT: Determine which version of BIND name daemon is running

```
BIND 'NAMED' is an open-source DNS server from ISC.org.
Many proprietary DNS servers are based on BIND source code.
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.
The remote bind version is : 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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10028

[return to 172.30.0.30]

2.1.25 Low general/SMBClient

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = UNIX
Domain = WORKGROUP
SMB Serverversion = SAMBA 3.0.20-DEBIAN
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = UNIX
Domain = WORKGROUP
SMB Serverversion = Samba 3.0.20-Debian
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = Unix
Domain = WORKGROUP
SMB Serverversion = SAMBA 3.0.20-DEBIAN
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

Low (CVSS: 0.0)
NVT: SMB Test

```
OS Version = Unix
Domain = WORKGROUP
SMB Serverversion = Samba 3.0.20-Debian
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90011

[return to 172.30.0.30]

2.1.26 Low telnet (23/tcp)

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

```
 Summary:
 A telnet Server is running at this host.
   Experts in computer security, such as SANS Institute, and the members of the
   comp.os.linux.security newsgroup recommend that the use of Telnet for remote
   logins should be discontinued under all normal circumstances, for the followi
↪ng
   reasons:
   * Telnet, by default, does not encrypt any data sent over the connection
     (including passwords), and so it is often practical to eavesdrop on the
     communications and use the password later for malicious purposes; anybody w
↪ho
     has access to a router, switch, hub or gateway located on the network betwe
↪en
     the two hosts where Telnet is being used can intercept the packets passing
↪by
     and obtain login and password information (and whatever else is typed) with
↪ any
```

... continues on next page ...

... continued from previous page ...

```
     of several common utilities like tcpdump and Wireshark.

   * Most implementations of Telnet have no authentication that would ensure
     communication is carried out between the two desired hosts and not intercep
↪ted
     in the middle.
   * Commonly used Telnet daemons have several vulnerabilities discovered over
     the years.



OID of test routine: 1.3.6.1.4.1.25623.1.0.100074
```

[return to 172.30.0.30]

2.1.27 Low tftp (69/udp)

Low (CVSS: 0.0)
NVT: TFTP detection

```
 Summary:
 The remote host has TFTP server running.
Description :
The remote host has TFTP server running. TFTP stands
for Trivial File Transfer Protocol.
 Solution:
 Disable TFTP server if not used.



OID of test routine: 1.3.6.1.4.1.25623.1.0.80100
```

[return to 172.30.0.30]

2.1.28 Low vnc (5900/tcp)

Low
NVT:

```
The remote VNC server chose security type #2 (VNC authentication)



OID of test routine: 1.3.6.1.4.1.25623.1.0.19288
```

[return to 172.30.0.30]

2.1.29 Log distcc (3632/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.30]

2.1.30 Log ftp (21/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
An FTP server is running on this port.
Here is its banner :
220 (vsFTPd 2.3.4)
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 172.30.0.30]

2.1.31 Log http (80/tcp)

Log
NVT:

. . . continues on next page . . .

. . . continued from previous page . . .

```
Open port.
```

OID of test routine: 0

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

```
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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10107

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

```
This are the directories/files found with brute force:
http://172.30.0.30:80/
http://172.30.0.30:80/cgi-bin/
http://172.30.0.30:80/dav/
http://172.30.0.30:80/doc/
http://172.30.0.30:80/icons/
http://172.30.0.30:80/index
http://172.30.0.30:80/index.php
http://172.30.0.30:80/index/
http://172.30.0.30:80/phpMyAdmin/
http://172.30.0.30:80/test/
http://172.30.0.30:80/phpMyAdmin/docs
http://172.30.0.30:80/phpMyAdmin/error
http://172.30.0.30:80/phpMyAdmin/error.php
http://172.30.0.30:80/phpMyAdmin/error/
http://172.30.0.30:80/phpMyAdmin/export
http://172.30.0.30:80/phpMyAdmin/export.php
http://172.30.0.30:80/phpMyAdmin/export/
http://172.30.0.30:80/phpMyAdmin/import
http://172.30.0.30:80/phpMyAdmin/import.php
http://172.30.0.30:80/phpMyAdmin/import/
http://172.30.0.30:80/phpMyAdmin/index
http://172.30.0.30:80/phpMyAdmin/index.php
http://172.30.0.30:80/phpMyAdmin/index/
```

. . . continues on next page . . .

... continued from previous page ...

```
http://172.30.0.30:80/phpMyAdmin/js/
http://172.30.0.30:80/phpMyAdmin/libraries/
http://172.30.0.30:80/phpMyAdmin/main
http://172.30.0.30:80/phpMyAdmin/main.php
http://172.30.0.30:80/phpMyAdmin/main/
http://172.30.0.30:80/phpMyAdmin/navigation
http://172.30.0.30:80/phpMyAdmin/navigation.php
http://172.30.0.30:80/phpMyAdmin/navigation/
http://172.30.0.30:80/phpMyAdmin/phpmyadmin
http://172.30.0.30:80/phpMyAdmin/phpmyadmin/
http://172.30.0.30:80/phpMyAdmin/print
http://172.30.0.30:80/phpMyAdmin/readme
http://172.30.0.30:80/phpMyAdmin/readme.php
http://172.30.0.30:80/phpMyAdmin/readme/
http://172.30.0.30:80/phpMyAdmin/scripts/
http://172.30.0.30:80/phpMyAdmin/setup/
http://172.30.0.30:80/phpMyAdmin/sql
http://172.30.0.30:80/phpMyAdmin/sql.php
http://172.30.0.30:80/phpMyAdmin/sql/
http://172.30.0.30:80/phpMyAdmin/test/
http://172.30.0.30:80/phpMyAdmin/webapp
http://172.30.0.30:80/phpMyAdmin/webapp.php
http://172.30.0.30:80/phpMyAdmin/webapp/
http://172.30.0.30:80/phpMyAdmin/setup/config
http://172.30.0.30:80/phpMyAdmin/setup/config.php
http://172.30.0.30:80/phpMyAdmin/setup/config/
http://172.30.0.30:80/phpMyAdmin/setup/index
http://172.30.0.30:80/phpMyAdmin/setup/index.php
http://172.30.0.30:80/phpMyAdmin/setup/index/
http://172.30.0.30:80/phpMyAdmin/setup/lib/
http://172.30.0.30:80/phpMyAdmin/setup/scripts
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103079

Log (CVSS: 0.0)
NVT: Services

```
A web server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Web mirroring

```
The following CGI have been discovered :
Syntax : cginame (arguments [default value])
/twiki/bin/edit/Sandbox/TestTopic3 (topicparent [Sandbox.WebHome] )
/twiki/bin/view/Know/WebChanges (topic [] )
/twiki/bin/edit/Know/WebPreferences (t [1444141981] )
/twiki/bin/edit/TWiki/GoodStyle (t [1444142004] )
/twiki/bin/view/Know/WebTopicList (topic [] skin [print] )
/twiki/bin/edit/Know/WebTopicList (t [1444142018] )
/twiki/bin/view/TWiki/TWikiPreferences (topic [] )
/twiki/bin/rdiff/Sandbox/WebIndex (rev1 [1.2] rev2 [1.1] )
/twiki/bin/view/Sandbox/WebNotify (topic [] skin [print] rev [1.4] )
/twiki/bin/edit/Sandbox/WebNotify (t [1444142026] )
/twiki/bin/view/Main/TWikiAdminGroup (topic [] skin [print] rev [1.6] )
/twiki/bin/oops/Main/TWikiAdminGroup (template [oopsmore] param1 [1.7] param2 [1
↪.7] )
/twiki/bin/edit/Main/PeterThoeny (t [1444142030] )
/twiki/bin/upload/Main/WebHome (filepath [] filecomment [] filename [] hidefile
↪[] createlink [] )
/twiki/bin/oops/Main/LondonOffice (template [oopsmore] param1 [1.3] param2 [1.3]
↪ )
/twiki/bin/rdiff/Main/WebStatistics (rev1 [1.6] rev2 [1.5] )
/twiki/bin/edit/Main/BookView (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/Main/WebTopicViewTemplate (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/Main/UnlockTopic (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/Main/DontNotify (topicparent [Main.TWikiVariables] )
/twiki/bin/oops/Main/KevinKinnell (param1 [1.2] param2 [1.2] template [oopsmore]
↪ )
/phpMyAdmin/phpmyadmin.css.php (token [36daaf86b57c7978c79de83f250e01a7] js_fram
↪e [right] lang [en-utf-8] nocache [2457687151] convcharset [utf-8] )
/mutillidae/index.php (username [anonymous] do [toggle-hints] page [home.php] )
/mutillidae/ (page [add-to-your-blog.php] )
/mutillidae/styles/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/twiki/bin/edit/Sandbox/TestTopic4 (topicparent [Sandbox.WebHome] )
/twiki/bin/view/Main/WebSearch (topic [] )
/twiki/bin/search/Main/ (showlock [] search [] web [] scope [topic] nosearch []
↪reverse [] regex [] order [] nototal [] limit [all] bookview [] nosummary [] c
↪asesensitive [] )
/twiki/bin/view/TWiki/TWikiTopics (topic [] )
/twiki/bin/view/TWiki/TWikiVariables (topic [] )
/twiki/bin/view/TWiki/InstantEnhancements (topic [] )
/twiki/bin/view/TWiki/WikiName (topic [] skin [print] rev [1.2] )
/twiki/bin/view/Sandbox/TestTopic2 (unlock [on] )
/twiki/bin/preview/Sandbox/TestTopic2 (formtemplate [] topicparent [] cmd [] )
/twiki/bin/upload/Main/TWikiGroups (filename [] filepath [] filecomment [] creat
↪elink [] hidefile [] )
```

... continues on next page ...

... continued from previous page ...

```
/twiki/bin/view/Main/WebStatistics (topic [] skin [print] rev [1.5] )
/twiki/bin/edit/Main/CoreTeam (topicparent [Main.AndreaSterbini] )
/twiki/bin/view/TWiki/WikiSyntax (topic [] skin [print] rev [1.14] )
/twiki/bin/edit/Sandbox/TestTopic5 (topicparent [Sandbox.WebHome] )
/twiki/bin/edit/Main/WebPreferences (t [1444141965] )
/twiki/bin/view/TWiki/WebChanges (topic [] )
/twiki/bin/view/TWiki/GoodStyle (topic [] skin [print] rev [1.5] )
/twiki/bin/oops/TWiki/DefaultPlugin (template [oopsmore] param1 [1.5] param2 [1.
↪5] )
/twiki/bin/view/TWiki/InterwikiPlugin (topic [] )
/twiki/bin/oops/Know/ReadmeFirst (template [oopsmore] param1 [1.6] param2 [1.6]
↪)
/twiki/bin/oops/Know/WebStatistics (template [oopsmore] param1 [1.4] param2 [1.4
↪] )
/twiki/bin/view/Sandbox/TestTopic3 (unlock [on] )
/twiki/bin/preview/Sandbox/TestTopic3 (formtemplate [] topicparent [] cmd [] )
/twiki/bin/rdiff/Sandbox/WebNotify (rev1 [1.5] rev2 [1.4] )
/twiki/bin/oops/TWiki/WikiCulture (template [oopsmore] param1 [1.8] param2 [1.8]
↪ )
/twiki/bin/edit/Main/TWikiGuest (t [1444142037] )
/twiki/bin/oops/Main/JohnTalintyre (template [oopsmore] param1 [1.3] param2 [1.3
↪] )
/twiki/bin/view/Main/TWikiVariables (topic [] skin [print] rev [1.2] )
/twiki/bin/view/TWiki/WikiWord (topic [] skin [print] rev [1.3] )
/twiki/bin/upload/Main/WebPreferences (filename [] filepath [] filecomment [] cr
↪eatelink [] hidefile [] )
/twiki/bin/edit/Sandbox/TestTopic6 (topicparent [Sandbox.WebHome] )
/twiki/bin/edit/Main/SupportGroup (topicparent [Main.TWikiGroups] )
/twiki/bin/view/TWiki/WebTopicList (topic [] )
/twiki/bin/edit/TWiki/TWikiShorthand (t [1444142006] )
/twiki/bin/rdiff/TWiki/TWikiGlossary (rev1 [1.2] rev2 [1.1] )
/twiki/bin/edit/TWiki/WikiStyleWord (topicparent [TWiki.TextFormattingFAQ] )
/twiki/bin/view/TWiki/InterWikis (topic [] )
/twiki/bin/view/TWiki/TWikiAdminCookBook (topic [] )
/twiki/bin/edit/Know/WebStatistics (t [1444142019] )
/twiki/bin/oops/Main/SanJoseOffice (template [oopsmore] param1 [1.3] param2 [1.3
↪] )
/twiki/bin/view/Main/TokyoOffice (topic [] skin [print] rev [1.2] )
/twiki/bin/rdiff/Main/WebNotify (rev1 [1.7] rev2 [1.6] )
/twiki/bin/oops/Main/WebNotify (template [oopsmore] param1 [1.7] param2 [1.7] )
/twiki/bin/rdiff/Main/NobodyGroup (rev1 [1.2] rev2 [1.1] )
/twiki/bin/edit/Main/JohnTalintyre (t [1444142042] )
/twiki/bin/rdiff/Main/AndreaSterbini (rev1 [1.2] rev2 [1.1] )
/twiki/bin/edit/TWiki/WikiSyntax (t [1444142054] )
/twiki/bin/upload/TWiki/WebHome (filepath [] filecomment [] filename [] hidefile
↪ [] createlink [] )
/twiki/bin/edit/Sandbox/TestTopic7 (topicparent [Sandbox.WebHome] )
```

... continues on next page ...

... continued from previous page ...

```
/twiki/bin/view/Main/TWikiGroups (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/Main/EngineeringGroup (topicparent [Main.TWikiGroups] )
/twiki/bin/search/Main/SearchResult (search [TWiki%20*Groups%5B%5EA-Za-z%5D] sco
↪pe [text] regex [on] )
/twiki/bin/register/Main/WebHome (Twk1Name [] Twk1WikiName [] Twk1LoginName [] T
↪wk1Email [] TwkOPhone [] TwkODepartment [] Twk1Location [] TopicName [TWikiReg
↪istration] )
/twiki/bin/edit/Sandbox/WebChanges (t [1444141984] )
/twiki/bin/edit/TWiki/TWikiSite (t [1444142002] )
/twiki/bin/rdiff/Know/WebStatistics (rev1 [1.4] rev2 [1.3] )
/twiki/bin/view/Sandbox/WebTopicList (topic [] skin [print] )
/twiki/bin/oops/Sandbox/WebTopicList (template [oopsmore] param1 [1.1] param2 [1
↪.1] )
/twiki/bin/view/Main/CharleytheHorse (topic [] skin [print] rev [r1.1] )
/twiki/bin/oops/Main/CharleytheHorse (param1 [1.1] param2 [1.1] template [oopsmo
↪re] )
/twiki/bin/rdiff/Main/PeterThoeny (rev1 [1.8] rev2 [1.7] )
/twiki/bin/edit/Main/SanJoseOffice (t [1444142033] )
/twiki/bin/view/Main/TWikiGuest (topic [] skin [print] rev [1.4] )
/twiki/bin/rdiff/Main/JohnTalintyre (rev1 [1.3] rev2 [1.2] )
/twiki/bin/attach/TWiki/FileAttachment (filename [Sample.txt] revInfo [1] )
/twiki/bin/oops/Main/GrantBow (param1 [1.1] param2 [1.1] template [oopsmore] )
/twiki/bin/rdiff/Main/MikeMannix (rev1 [1.5] rev2 [1.4] )
/twiki/bin/edit/Sandbox/TestTopic8 (topicparent [Sandbox.WebHome] )
/twiki/bin/search/Sandbox/SearchResult (search [] nosearch [on] scope [topic] re
↪verse [on] regex [on] order [modified] )
/twiki/bin/view/Main/OfficeLocations (topic [] skin [print] rev [1.3] )
/twiki/bin/oops/Main/OfficeLocations (template [oopsmore] param1 [1.4] param2 [1
↪.4] )
/twiki/bin/edit/TWiki/StartingPoints (t [1444141971] )
/twiki/bin/rdiff/TWiki/StartingPoints (rev1 [1.3] rev2 [1.2] )
/twiki/bin/rdiff/Sandbox/WebChanges (rev1 [1.2] rev2 [1.1] )
/phpMyAdmin/themes/original/img/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/twiki/bin/view/TWiki/TWikiTutorial (topic [] )
/twiki/bin/edit/TWiki/MeaningfulTitle (topicparent [TWiki.TextFormattingFAQ] )
/twiki/bin/view/Know/WebIndex (topic [] )
/twiki/bin/view/Know/WebStatistics (topic [] skin [print] rev [1.3] )
/twiki/bin/oops/Sandbox/WebIndex (template [oopsmore] param1 [1.2] param2 [1.2]
↪)
/twiki/bin/edit/TWiki/WikiName (t [1444142022] )
/twiki/bin/view/Sandbox/WebStatistics (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/Sandbox/WebStatistics (t [1444142026] )
/twiki/bin/rdiff/Sandbox/WebStatistics (rev1 [1.3] rev2 [1.2] )
/twiki/bin/oops/Sandbox/WebStatistics (template [oopsmore] param1 [1.3] param2 [
↪1.3] )
/twiki/bin/rdiff/Main/SanJoseOffice (rev1 [1.3] rev2 [1.2] )
/twiki/bin/edit/Main/TokyoOffice (t [1444142035] )
```

... continues on next page ...

. . . continued from previous page . . .

```
/twiki/bin/view/Main/JohnTalintyre (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/Main/TWikiVariables (t [1444142042] )
/twiki/bin/oops/Main/MikeMannix (template [oopsmore] param1 [1.5] param2 [1.5] )
/twiki/bin/view/TWiki/BookView (topic [] skin [print] rev [1.1] )
/twiki/bin/edit/TWiki/WikiReferences (t [1444142053] )
/twiki/bin/rdiff/TWiki/WikiReferences (rev1 [1.2] rev2 [1.1] )
/twiki/bin/view/TWiki/WebHome (topic [] )
/twiki/bin/search/TWiki/ (showlock [] search [] web [] nosearch [] scope [topic]
↪ reverse [] regex [] limit [all] nototal [] order [] nosummary [] bookview []
↪casesensitive [] )
/twiki/bin/edit/Main/TWikiGroups (t [1444141953] )
/twiki/bin/view/TWiki/WelcomeGuest (topic [] )
/twiki/bin/view/TWiki/TWikiRegistration (topic [] skin [print] rev [1.7] )
/twiki/bin/edit/TWiki/TWikiRegistration (t [1444141968] )
/twiki/bin/rdiff/TWiki/TWikiRegistration (rev1 [1.8] rev2 [1.7] )
/twiki/bin/oops/TWiki/TWikiRegistration (template [oopsmore] param1 [1.8] param2
↪ [1.8] )
/twiki/bin/view/Sandbox/WebChanges (topic [] skin [print] )
/twiki/bin/view/TWiki/TWikiSite (topic [] skin [print] )
/twiki/bin/edit/TWiki/NewTopic (topicparent [TWiki.TWikiShorthand] )
/twiki/bin/oops/TWiki/TWikiGlossary (template [oopsmore] param1 [1.2] param2 [1.
↪2] )
/twiki/bin/view/TWiki/DefaultPlugin (topic [] skin [print] rev [1.4] )
/twiki/bin/edit/TWiki/WikiOrg (topicparent [TWiki.TWikiAdminCookBook] )
/twiki/bin/view/Know/WebNotify (topic [] skin [print] rev [1.6] )
/twiki/bin/oops/Sandbox/WebNotify (template [oopsmore] param1 [1.5] param2 [1.5]
↪ )
/twiki/bin/view/Main/SanJoseOffice (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/TWiki/TWikiFormTemplate (topicparent [Main.WebPreferences] )
/twiki/bin/oops/Main/AndreaSterbini (param1 [1.2] param2 [1.2] template [oopsmor
↪e] )
/twiki/bin/edit/TWiki/WikiWord (t [1444142051] )
/twiki/bin/edit/TWiki/StandardColors (t [1444142055] )
/twiki/bin/rdiff/TWiki/StandardColors (rev1 [1.4] rev2 [1.3] )
/twiki/bin/rdiff/TWiki/SiteMap (rev1 [1.2] rev2 [1.1] )
/twiki/bin/view/TWiki/WebTopicEditTemplate (topic [] skin [print] rev [1.4] )
/twiki/bin/edit/TWiki/WebTopicEditTemplate (t [1444142057] )
/twiki/bin/rdiff/TWiki/WebTopicEditTemplate (rev1 [1.5] rev2 [1.4] )
/twiki/bin/oops/TWiki/WebTopicEditTemplate (template [oopsmore] param1 [1.5] par
↪am2 [1.5] )
/twiki/bin/upload/TWiki/TWikiRegistration (filename [] filepath [] filecomment [
↪] createlink [] hidefile [] )
/twiki/bin/edit/TWiki/WebPreferences (t [1444141975] )
/twiki/bin/rdiff/Know/WebPreferences (rev1 [1.11] rev2 [1.10] )
/twiki/bin/view/Main/GrantBow (topic [] skin [print] rev [r1.1] )
/twiki/bin/rdiff/TWiki/WikiSyntax (rev1 [1.15] rev2 [1.14] )
/twiki/bin/edit/TWiki/SiteMap (t [1444142056] )
```

. . . continues on next page . . .

... continued from previous page ...

```
/dav/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/mutillidae/styles/ddsmoothmenu/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/twiki/bin/view/TWiki/WebSearch (topic [] )
/twiki/bin/search/Sandbox/ (search [%5C.*] web [] nosearch [on] scope [topic] re
↪verse [on] regex [on] nototal [] limit [100] order [modified] nosummary [] boo
↪kview [] casesensitive [] )
/twiki/bin/view/Sandbox/WebSearch (topic [] )
/twiki/bin/view/TWiki/TextFormattingRules (topic [] )
/twiki/bin/view/TWiki/TextFormattingFAQ (topic [] )
/twiki/bin/view/Know/ReadmeFirst (topic [] skin [print] rev [1.5] )
/twiki/bin/preview/Sandbox/WebHome (formtemplate [] topicparent [] cmd [] )
/twiki/bin/edit/Main/TWikiRegistration (topicparent [Main.OfficeLocations] )
/twiki/bin/oops/Main/NobodyGroup (param1 [1.2] param2 [1.2] template [oopsmore]
↪)
/twiki/bin/edit/Main/WebTopicNonWikiTemplate (topicparent [Main.TWikiVariables]
↪)
/twiki/bin/edit/Main/TWikiDocumentation (topicparent [Main.FileAttachment] )
/twiki/bin/edit/Main/MikeMannix (t [1444142048] )
/twiki/bin/edit/TWiki/YearTwoThousand (topicparent [TWiki.WikiWord] )
/twiki/bin/rdiff/Main/WebPreferences (rev1 [1.13] rev2 [1.12] )
/twiki/bin/search/TWiki/SearchResult (search [TWiki%20*Registration%5B%5EA-Za-z%
↪5D] scope [text] regex [on] )
/twiki/bin/search/Know/ (search [%54opicClassification.%2ANoDisclosure] web [] s
↪cope [text] regex [on] bookview [] )
/twiki/bin/edit/TWiki/DefaultPlugin (t [1444142013] )
/twiki/bin/edit/Main/TWikiAdminGroup (t [1444142028] )
/twiki/bin/rdiff/Main/TWikiAdminGroup (rev1 [1.7] rev2 [1.6] )
/twiki/bin/oops/Main/PeterThoeny (template [oopsmore] param1 [1.8] param2 [1.8]
↪)
/twiki/bin/rdiff/Main/TokyoOffice (rev1 [1.3] rev2 [1.2] )
/twiki/bin/edit/Main/IncludeTopicsAndWebPages (topicparent [Main.TWikiVariables]
↪ )
/twiki/bin/edit/Main/TWikiForms (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/Main/FormattedSearch (topicparent [Main.TWikiVariables] )
/twiki/bin/edit/TWiki/BookView (t [1444142049] )
/twiki/bin/edit/TWiki/AVeryLongWikiTopicNameIsAlsoPossible (topicparent [TWiki.W
↪ikiWord] )
/twiki/bin/rdiff/Main/TWikiGroups (rev1 [1.3] rev2 [1.2] )
/twiki/bin/oops/Know/WebPreferences (template [oopsmore] param1 [1.11] param2 [1
↪.11] )
/twiki/bin/view/TWiki/WebChangesAlert (topic [] skin [print] rev [1.12] )
/twiki/bin/edit/TWiki/WebChangesAlert (t [1444142009] )
/twiki/bin/rdiff/TWiki/WebChangesAlert (rev1 [1.13] rev2 [1.12] )
/twiki/bin/oops/TWiki/WebChangesAlert (template [oopsmore] param1 [1.13] param2
↪[1.13] )
/twiki/bin/rename/TWiki/WebChangesAlert (newweb [TWiki] newtopic [WebChangesNoti
↪fy] confirm [on] )
```

... continues on next page ...

. . . continued from previous page . . .

```
/twiki/bin/view/TWiki/TWikiGlossary (topic [] skin [print] rev [1.1] )
/twiki/bin/edit/Know/ReadmeFirst (t [1444142016] )
/twiki/bin/edit/Know/WebNotify (t [1444142018] )
/twiki/bin/view/Main/WebNotify (topic [] skin [print] rev [1.6] )
/twiki/bin/view/Main/AndreaSterbini (topic [] skin [print] rev [1.1] )
/twiki/bin/view/Main/MikeMannix (topic [] skin [print] rev [1.4] )
/twiki/bin/oops/TWiki/WikiNotation (template [oopsmore] param1 [1.3] param2 [1.3
↪] )
/twiki/bin/view/Main/TWikiUsers (topic [] rev [r1.15] )
/twiki/bin/view/TWiki/WebIndex (topic [] )
/twiki/bin/view/TWiki/TWikiShorthand (topic [] skin [print] )
/twiki/bin/oops/TWiki/TWikiShorthand (template [oopsmore] param1 [1.1] param2 [1
↪.1] )
/twiki/bin/view/TWiki/TWikiFAQ (topic [] )
/twiki/bin/view/Sandbox/WebIndex (topic [] skin [print] rev [1.1] )
/twiki/bin/rdiff/TWiki/WikiName (rev1 [1.3] rev2 [1.2] )
/twiki/bin/oops/TWiki/WikiName (template [oopsmore] param1 [1.3] param2 [1.3] )
/twiki/bin/view/Main/LondonOffice (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/Main/LondonOffice (t [1444142034] )
/twiki/bin/view/Main/KevinKinnell (topic [] skin [print] rev [1.1] )
/twiki/bin/edit/Main/KevinKinnell (t [1444142044] )
/twiki/bin/view/TWiki/RegularExpression (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/TWiki/RegularExpression (t [1444142050] )
/twiki/bin/rdiff/TWiki/RegularExpression (rev1 [1.3] rev2 [1.2] )
/twiki/bin/oops/TWiki/RegularExpression (template [oopsmore] param1 [1.3] param2
↪ [1.3] )
/twiki/bin/view/TWiki/FormattedSearch (topic [] )
/twiki/bin/edit/TWiki/WikiNotation (t [1444142058] )
/twiki/bin/view/TWiki/FileAttachment (topic [] )
/twiki/bin/rdiff/Main/TWikiVariables (rev1 [1.3] rev2 [1.2] )
/twiki/bin/edit/Main/WikiSyntax (topicparent [Main.TWikiVariables] )
/twiki/bin/viewfile/TWiki/FileAttachment (rev [] filename [Sample.txt] )
/twiki/bin/rdiff/TWiki/WikiWord (rev1 [1.4] rev2 [1.3] )
/twiki/bin/oops/TWiki/WikiWord (template [oopsmore] param1 [1.4] param2 [1.4] )
/twiki/bin/oops/TWiki/WikiSyntax (template [oopsmore] param1 [1.15] param2 [1.15
↪] )
/twiki/bin/rdiff/TWiki/WikiNotation (rev1 [1.3] rev2 [1.2] )
/twiki/bin/search/Know/SearchResult (search [] scope [text] regex [on] )
/twiki/bin/view/TWiki/StartingPoints (topic [] skin [print] rev [1.2] )
/twiki/bin/oops/TWiki/StartingPoints (template [oopsmore] param1 [1.3] param2 [1
↪.3] )
/twiki/bin/rdiff/TWiki/GoodStyle (rev1 [1.6] rev2 [1.5] )
/twiki/bin/edit/TWiki/TWikiGlossary (t [1444142010] )
/twiki/bin/edit/Sandbox/WebIndex (t [1444142021] )
/twiki/bin/edit/Sandbox/WebTopicList (t [1444142025] )
/twiki/bin/edit/Main/CharleytheHorse (t [1444142027] )
/twiki/bin/view/TWiki/WikiCulture (topic [] skin [print] rev [1.7] )
```

. . . continues on next page . . .

... continued from previous page ...

```
/twiki/bin/edit/TWiki/WikiCulture (t [1444142029] )
/twiki/bin/rdiff/Main/LondonOffice (rev1 [1.3] rev2 [1.2] )
/twiki/bin/view/Main/WebRss (topic [] rev [r1.1] )
/twiki/bin/edit/Main/RegularExpression (topicparent [Main.TWikiVariables] )
/twiki/bin/rdiff/Main/KevinKinnell (rev1 [1.2] rev2 [1.1] )
/twiki/bin/edit/Main/AndreaSterbini (t [1444142045] )
/twiki/bin/view/Main/FileAttachment (topic [] rev [r1.3] )
/twiki/bin/view/TWiki/WikiReferences (topic [] skin [print] rev [1.1] )
/twiki/bin/oops/TWiki/WikiReferences (template [oopsmore] param1 [1.2] param2 [1
↪.2] )
/twiki/bin/view/TWiki/WikiNotation (topic [] skin [print] rev [1.2] )
/twiki/bin/edit/Main/OfficeLocations (t [1444141958] )
/twiki/bin/rdiff/Main/OfficeLocations (rev1 [1.4] rev2 [1.3] )
/twiki/bin/view/Main/WebIndex (topic [] )
/twiki/bin/view/Know/WebSearch (topic [] )
/twiki/bin/view/Know/WebPreferences (topic [] skin [print] rev [1.10] )
/mutillidae/images/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/twiki/bin/edit/TWiki/TWikiTopic (topicparent [TWiki.TWikiTopics] )
/twiki/bin/oops/TWiki/GoodStyle (template [oopsmore] param1 [1.6] param2 [1.6] )
/twiki/bin/rdiff/Know/ReadmeFirst (rev1 [1.6] rev2 [1.5] )
/twiki/bin/oops/Main/TokyoOffice (template [oopsmore] param1 [1.3] param2 [1.3]
↪)
/twiki/bin/upload/Main/OfficeLocations (filename [] filepath [] filecomment [] c
↪reatelink [] hidefile [] )
/twiki/bin/edit/Main/WebNotify (t [1444142039] )
/twiki/bin/view/Main/NobodyGroup (topic [] skin [print] rev [1.1] )
/twiki/bin/view/TWiki/StandardColors (topic [] skin [print] rev [1.3] )
/twiki/bin/oops/TWiki/StandardColors (template [oopsmore] param1 [1.4] param2 [1
↪.4] )
/twiki/bin/view/Main/WebHome (topic [] rev [r1.20] )
/twiki/bin/view/Sandbox/WebHome (topic [] unlock [on] )
/twiki/bin/edit/Sandbox/TestTopic1 (topicparent [Sandbox.WebHome] )
/twiki/bin/oops/Main/TWikiGroups (template [oopsmore] param1 [1.3] param2 [1.3]
↪)
/twiki/bin/view/Main/WebChanges (topic [] )
/twiki/bin/edit/Main/WebTopicEditTemplate (topicparent [Main.WebPreferences] )
/twiki/bin/view/TWiki/WebPreferences (topic [] skin [print] )
/twiki/bin/view/TWiki/TWikiForms (topic [] )
/twiki/bin/edit/Sandbox/WebTopicEditTemplate (topicparent [Sandbox.WebPreference
↪s] )
/twiki/bin/view/TWiki/TWikiAccessControl (topic [] )
/twiki/bin/rdiff/TWiki/WikiCulture (rev1 [1.8] rev2 [1.7] )
/twiki/bin/view/Main/PeterThoeny (topic [] skin [print] rev [1.7] )
/twiki/bin/oops/Main/WebStatistics (template [oopsmore] param1 [1.6] param2 [1.6
↪] )
/twiki/bin/rdiff/Main/TWikiGuest (rev1 [1.5] rev2 [1.4] )
/twiki/bin/oops/Main/TWikiVariables (template [oopsmore] param1 [1.3] param2 [1.
```

... continues on next page ...

... continued from previous page ...

```
↪3] )
/twiki/bin/rdiff/TWiki/BookView (rev1 [1.2] rev2 [1.1] )
/twiki/bin/oops/TWiki/BookView (template [oopsmore] param1 [1.2] param2 [1.2] )
/twiki/bin/view/TWiki/SiteMap (topic [] skin [print] rev [1.1] )
/phpMyAdmin/index.php (phpMyAdmin [2ea6ffe2717b976a406f711eba7f64b437815015] tok
↪en [36daaf86b57c7978c79de83f250e01a7] pma_username [] table [] lang [] server
↪[1] db [] convcharset [utf-8] pma_password [] )
/twiki/bin/view/Know/WebHome (topic [] )
/twiki/bin/edit/Sandbox/TestTopic2 (topicparent [Sandbox.WebHome] )
/twiki/bin/view/Main/WebPreferences (topic [] skin [print] rev [1.12] )
/twiki/bin/view/Sandbox/WebPreferences (topic [] skin [print] rev [1.9] )
/twiki/bin/edit/Sandbox/WebPreferences (t [1444141988] )
/twiki/bin/rdiff/Sandbox/WebPreferences (rev1 [1.10] rev2 [1.9] )
/twiki/bin/oops/Sandbox/WebPreferences (template [oopsmore] param1 [1.10] param2
↪ [1.10] )
/twiki/bin/rdiff/TWiki/DefaultPlugin (rev1 [1.5] rev2 [1.4] )
/twiki/bin/rdiff/Know/WebNotify (rev1 [1.7] rev2 [1.6] )
/twiki/bin/oops/Know/WebNotify (template [oopsmore] param1 [1.7] param2 [1.7] )
/twiki/bin/edit/Main/WebStatistics (t [1444142036] )
/twiki/bin/oops/Main/TWikiGuest (template [oopsmore] param1 [1.5] param2 [1.5] )
/twiki/bin/edit/Main/NobodyGroup (t [1444142041] )
/twiki/bin/edit/Main/GrantBow (t [1444142047] )
Directory index found at /dav/
Directory index found at /twiki/TWikiDocumentation.html
Directory index found at /phpMyAdmin/themes/original/img/
Directory index found at /mutillidae/styles/
Directory index found at /mutillidae/styles/ddsmoothmenu/
Directory index found at /mutillidae/images/
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10662

Log (CVSS: 0.0)
NVT: Directory Scanner

```
The following directories were discovered:
/cgi-bin, /doc, /test, /icons, /phpMyAdmin
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11032

... continues on next page ...

. . . continued from previous page . . .

References

```
Other:
  OWASP:OWASP-CM-006
```

Log (CVSS: 0.0)
NVT: PHP Version Detection

```
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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.800109

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

```
wapiti report filename is empty. that could mean that
wrong version of wapiti is used or tmp dir is not accessible.
Make sure to have wapiti 2.x as wapiti 1.x is not supported.
In short: check installation of wapiti and OpenVAS
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

Log (CVSS: 0.0)
NVT: phpMyAdmin Detection

```
Detected phpMyAdmin version: unknown
Location: /phpMyAdmin
CPE: cpe:/a:phpmyadmin:phpmyadmin
Concluded from version identification result:
unknown
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900129

Log
NVT:

```
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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900498

Log (CVSS: 0.0)
NVT: TikiWiki Version Detection

```
Detected TikiWiki version: 1.9.5 under /tikiwiki
Location: /tikiwiki
CPE: cpe:/a:tikiwiki:tikiwiki:1.9.5
Concluded from version identification result:
1.9.5
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.901001

[return to 172.30.0.30]

2.1.32 Log mysql (3306/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

```
Detected MySQL version: 5.0.51a-3ubuntu5
Location: 3306/tcp
CPE: cpe:/a:mysql:mysql:5.0.51a
```

... continues on next page ...

... continued from previous page ...

Concluded from version identification result:
5.0.51a-3ubuntu5 ,G‘.c)@E ,ª zX,l_wX20:qL

OID of test routine: 1.3.6.1.4.1.25623.1.0.100152

Log (CVSS: 0.0)
NVT: Services

An unknown service is running on this port.
It is usually reserved for MySQL

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

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

MySQL can be accessed by remote attackers

OID of test routine: 1.3.6.1.4.1.25623.1.0.902799

References
Other:
URL:https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

[return to 172.30.0.30]

2.1.33 Log postgresql (5432/tcp)

Log
NVT:

Open port.

OID of test routine: 0

Log (CVSS: 0.0)
NVT: PostgreSQL Detection

```
Detected PostgreSQL version: 8.3.1
Location: 5432/tcp
CPE: cpe:/a:postgresql:postgresql:8.3.1
Concluded from version identification result:
T versionDg]PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.
↪3 (Ubuntu 4.2.3-2ubuntu4)CSELECTZI
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100151

Log (CVSS: 0.0)
NVT: Services

```
An unknown service is running on this port.
It is usually reserved for Postgres
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

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

```
Postgresql database can be accessed by remote attackers
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902799

References

```
Other:
  URL:https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_d
↪ss_v1-2.pdf
```

[return to 172.30.0.30]

2.1.34 Log scientia-ssdb (2121/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Services

```
An FTP server is running on this port.
Here is its banner :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.30.0.30]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 172.30.0.30]

2.1.35 Log ssh (22/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100259

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10267

Log (CVSS: 0.0)
NVT: Services

```
An ssh server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 172.30.0.30]

2.1.36 Log x11 (6000/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.30]

2.1.37 Log exec (512/tcp)

Log
NVT:

. . . continues on next page . . .

... continued from previous page ...

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.30]

2.1.38 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

```
ICMP based OS fingerprint results: (91% confidence)
Linux Kernel
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102002

References

```
Other:
  URL:http://www.phrack.org/issues.html?issue=57&amp;id=7#article
```

Log (CVSS: 0.0)
NVT: Checks for open udp ports

```
Open UDP ports: [None found]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103978

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

```
Arachni could not be found in your system path.
OpenVAS was unable to execute Arachni and to perform the scan you
requested.
Please make sure that Arachni is installed and that arachni is
available in the PATH variable defined for your environment.
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.110001

Log (CVSS: 0.0)
NVT: Traceroute

```
Here is the route from 172.30.0.7 to 172.30.0.30:
172.30.0.7
172.30.0.30
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Log (CVSS: 0.0)
NVT: TWiki Version Detection

```
Detected TWiki version: unknown
Location: /twiki
CPE:
Concluded from version identification result:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.800399

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

```
SMB signing is disabled on this host
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802726

Log (CVSS: 0.0)
NVT: Checks for open tcp ports

```
Open TCP ports: 80, 3632, 5900, 8009, 8787, 6667, 445, 21, 111, 2049, 22, 6000,
↪23, 512, 513, 25, 514, 1099, 2121, 3306, 139, 1524, 53, 5432
```

... continues on next page ...

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

Log (CVSS: 0.0)
NVT: Anonymous FTP Checking

```
Summary:
This FTP Server allows anonymous logins.
 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.
Solution:
If you do not want to share files, you should disable anonymous logins.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900600

References
CVE: CVE-1999-0497

[return to 172.30.0.30]

2.1.39 Log netbios-ssn (139/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SMB on port 445

```
An SMB server is running on this port
```

... continues on next page ...

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.11011

[return to 172.30.0.30]

2.1.40 Log shell (514/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.30]

2.1.41 Log smtp (25/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

```
Remote SMTP server banner :
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
This is probably: Postfix
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10263

Log (CVSS: 0.0)
NVT: SMTP STARTTLS Detection Detection

. . . continues on next page . . .

. . . continued from previous page . . .

```
Summary:
The remote Mailserver supports the STARTTLS command.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103118

Log (CVSS: 0.0)
NVT: Services

```
An SMTP server is running on this port
Here is its banner :
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 172.30.0.30]

2.1.42 Log domain (53/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: DNS Server Detection

```
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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 172.30.0.30]

2.1.43 Log telnet (23/tcp)

Log
NVT:

```
Open port.



OID of test routine: 0
```

Log (CVSS: 0.0)
NVT: Detect Server type and version via Telnet

```
Remote telnet banner :
                  _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:



OID of test routine: 1.3.6.1.4.1.25623.1.0.10281
```

Log (CVSS: 0.0)
NVT: Services

```
A telnet server seems to be running on this port



...continues on next page ...
```

. . . continued from previous page . . .

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 172.30.0.30]

2.1.44 Log vnc (5900/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.30]

2.1.45 Log ajp13 (8009/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

```
Nmap service detection result for this port: ajp13
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.30]

2.1.46 Log domain (53/udp)

Log (CVSS: 0.0)
NVT: DNS Server Detection

```
 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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 172.30.0.30]

2.1.47 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
172.30.0.30|cpe:/a:samba:samba:3.0.20
172.30.0.30|cpe:/a:postgresql:postgresql:8.3.1
172.30.0.30|cpe:/o:linux:kernel
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 172.30.0.30]

2.1.48 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:172.30.0.7,172.30.0.30
TCP ports:80,3632,5900,8009,8787,6667,445,21,111,2049,22,6000,23,512,513,25,514,
↪1099,2121,3306,139,1524,53,5432
UDP ports:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 172.30.0.30]

2.1.49 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. OID of test routine: 1.3.6.1.4.1.25623.1.0.103190
References CVE: CVE-1999-0524 Other: URL:http://www.ietf.org/rfc/rfc0792.txt

[return to 172.30.0.30]

2.1.50 Log ingreslock (1524/tcp)

Log NVT:
Open port. OID of test routine: 0

Log (CVSS: 0.0) NVT: Identify unknown services with nmap
Nmap service detection result for this port: shell OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.30]

2.1.51 Log ircd (6667/tcp)

Log NVT:
`Open port.` OID of test routine: 0

Log (CVSS: 0.0) NVT: Identify unknown services with nmap
`Nmap service detection result for this port: irc` OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.30]

2.1.52 Log login (513/tcp)

Log NVT:
`Open port.` OID of test routine: 0

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

`Nmap service detection result for this port: login`
`This is a guess. A confident identification of the service was not possible.`
 	
OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.30]

2.1.53 Log microsoft-ds (445/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

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.Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.0.20-Debian
Detected OS: Unix
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102011

Log (CVSS: 0.0)
NVT: SMB log in

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.10394

Log (CVSS: 0.0)
NVT: SMB on port 445

```
A CIFS server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11011

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

```
The following shares where found
IPC$
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902425

[return to 172.30.0.30]

2.1.54 Log msgsrvr (8787/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.30]

2.1.55 Log netbios-ns (137/udp)

Log (CVSS: 0.0)
NVT: Using NetBIOS to retrieve information from a Windows host

```
The following 7 NetBIOS names have been gathered :
 METASPLOITABLE  = This is the computer name registered for workstation services
↪ by a WINS client.
 METASPLOITABLE  = This is the current logged in user registered for this workst
↪ation.
```

. . . continues on next page . . .

... continued from previous page ...

```
 METASPLOITABLE  = Computer name
   __MSBROWSE__
 WORKGROUP       = Workgroup / Domain name
 WORKGROUP
 WORKGROUP       = Workgroup / Domain name (part of the Browser elections)
. This SMB server seems to be a SAMBA server (this is not a security
risk, this is for your information). This can be told because this server
claims to have a null MAC address
If you do not want to allow everyone to find the NetBios name
of your computer, you should filter incoming traffic to this port.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10150

[return to 172.30.0.30]

2.1.56 Log nfs (2049/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

[return to 172.30.0.30]

2.1.57 Log rmiregistry (1099/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

... continues on next page ...

... continued from previous page ...

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

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

OID of test routine: 1.3.6.1.4.1.25623.1.0.66286

[return to 172.30.0.30]

2.1.58 Log sunrpc (111/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: rpcinfo -p

```
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 35258/TCP
RPC program #100005 version 2 'mountd' (mount showmount) on port 35258/TCP
RPC program #100005 version 3 'mountd' (mount showmount) on port 35258/TCP
RPC program #100021 version 1 'nlockmgr' on port 51805/TCP
RPC program #100021 version 3 'nlockmgr' on port 51805/TCP
RPC program #100021 version 4 'nlockmgr' on port 51805/TCP
RPC program #100024 version 1 'status' on port 54725/TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/UDP
RPC program #100024 version 1 'status' on port 35332/UDP
```

... continues on next page ...

. . . continued from previous page . . .

```
RPC program #100005 version 1 'mountd' (mount showmount) on port 41994/UDP
RPC program #100005 version 2 'mountd' (mount showmount) on port 41994/UDP
RPC program #100005 version 3 'mountd' (mount showmount) on port 41994/UDP
RPC program #100021 version 1 'nlockmgr' on port 44356/UDP
RPC program #100021 version 3 'nlockmgr' on port 44356/UDP
RPC program #100021 version 4 'nlockmgr' on port 44356/UDP
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11111

[return to 172.30.0.30]
