

Scan Report

May 11, 2017

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Metasploitable2_{Authenticated}final”. These 47 : 392017UTC and ended at Thu May 11 16 : 48 : 29 2017 UTC. The report first summarises the results found. Then, for each host,

Contents

1	Result Overview	2
1.1	Host Authentications	2
2	Results per Host	2
2.1	192.168.8.102	2
2.1.1	High 1524/tcp	3
2.1.2	High 8787/tcp	3
2.1.3	High 5432/tcp	5
2.1.4	High 21/tcp	6
2.1.5	High 3632/tcp	7
2.1.6	High 80/tcp	8
2.1.7	High 6200/tcp	15
2.1.8	High 5900/tcp	16
2.1.9	High 1099/tcp	17
2.1.10	High general/tcp	18
2.1.11	Medium 6667/tcp	18
2.1.12	Medium 445/tcp	19
2.1.13	Medium 5432/tcp	20
2.1.14	Medium 21/tcp	33
2.1.15	Medium 80/tcp	34
2.1.16	Medium 22/tcp	49
2.1.17	Low 5432/tcp	50
2.1.18	Low 22/tcp	52
2.1.19	Low general/tcp	53

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.8.102	19	34	4	0	0
Total: 1	19	34	4	0	0

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found.

It only lists hosts that produced issues.

Issues with the threat level “Log” are not shown.

Issues with the threat level “Debug” are not shown.

Issues with the threat level “False Positive” are not shown.

Only results with a minimum QoD of 70 are shown.

This report contains all 57 results selected by the filtering described above. Before filtering there were 290 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.8.102	SSH	Failure	Protocol SSH, Port 22, User msfadmin : Login failure
192.168.8.102	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.8.102

Host scan start Thu May 11 15:48:15 2017 UTC

Host scan end Thu May 11 16:48:29 2017 UTC

Service (Port)	Threat Level
1524/tcp	High
8787/tcp	High
5432/tcp	High
21/tcp	High
3632/tcp	High
80/tcp	High
6200/tcp	High
5900/tcp	High
1099/tcp	High

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
general/tcp	High
6667/tcp	Medium
445/tcp	Medium
5432/tcp	Medium
21/tcp	Medium
80/tcp	Medium
22/tcp	Medium
5432/tcp	Low
22/tcp	Low
general/tcp	Low

2.1.1 High 1524/tcp

High (CVSS: 10.0) NVT: Possible Backdoor: Ingreslock
Summary A backdoor is installed on the remote host
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.
Solution Solution type: Workaround
Vulnerability Detection Method Details:Possible Backdoor: Ingreslock OID:1.3.6.1.4.1.25623.1.0.103549 Version used: \$Revision: 4718 \$

[\[return to 192.168.8.102 \]](#)**2.1.2 High 8787/tcp**

High (CVSS: 10.0) NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities
Summary ... continues on next page ...

...continued from previous page ...
Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.
<p>Vulnerability Detection Result</p> <p>The service is running in \$SAFE >= 1 mode. However it is still possible to run a ↵bitrary syscall commands on the remote host. Sending an invalid syscall the s ↵ervice returned the following response:</p> <pre>Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'syscall'"0/usr/lib/ ↵ruby/1.8/drb/drb.rb:1555:in 'send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in '__se ↵nd__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in 'perform_without_block'"3/usr/lib/ ↵ruby/1.8/drb/drb.rb:1515:in 'perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in 'm ↵ain_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in 'loop'"5/usr/lib/ruby/1.8/drb/ ↵drb.rb:1585:in 'main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in 'start'"5/usr ↵/lib/ruby/1.8/drb/drb.rb:1581:in 'main_loop'"/usr/lib/ruby/1.8/drb/drb.rb:143 ↵0:in 'run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in 'start'"/usr/lib/ruby/1.8/dr ↵b/drb.rb:1427:in 'run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in 'initialize'"/us ↵r/lib/ruby/1.8/drb/drb.rb:1627:in 'new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in ↵'start_service'"/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im ↵plemented</pre>
<p>Impact</p> <p>By default, Distributed Ruby does not impose restrictions on allowed hosts or set the \$SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.</p>
<p>Solution</p> <p>Solution type: Mitigation</p> <p>Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:</p> <ul style="list-style-type: none"> - Implementing taint on untrusted input - Setting \$SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate) - Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts
<p>Vulnerability Detection Method</p> <p>Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.</p> <p>Details:Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.108010 Version used: \$Revision: 4387 \$</p>
<p>References</p> <p>BID:47071</p> <p>Other:</p> <p>URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=22750</p>
...continues on next page ...

...continued from previous page ...
URL:http://www.securityfocus.com/bid/47071
URL:http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_t
↔esters/
URL:http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html

[[return to 192.168.8.102](#)]

2.1.3 High 5432/tcp

High (CVSS: 9.0) NVT: PostgreSQL weak password
Summary It was possible to login into the remote PostgreSQL as user postgres using weak credentials.
Vulnerability Detection Result It was possible to login as user postgres with password "postgres".
Solution Change the password as soon as possible.
Vulnerability Detection Method Details:PostgreSQL weak password OID:1.3.6.1.4.1.25623.1.0.103552 Version used: \$Revision: 5888 \$

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
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution ... continues on next page ...

...continued from previous page ...
Updates are available. Please see the references for more information.
Vulnerability Detection Method Details:PostgreSQL Multiple Security Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100645 Version used: \$Revision: 5373 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2010-1169, CVE-2010-1170, CVE-2010-1447 BID:40215 Other: URL:http://www.securityfocus.com/bid/40215 URL:http://www.postgresql.org/about/news.1203 URL:http://www.postgresql.org/ URL:http://www.postgresql.org/support/security

[\[return to 192.168.8.102 \]](#)

2.1.4 High 21/tcp

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

...continued from previous page...

Vulnerability Detection Method

Details:vsftpd Compromised Source Packages Backdoor Vulnerability

OID:1.3.6.1.4.1.25623.1.0.103185

Version used: \$Revision: 5026 \$

References

BID:48539

Other:

URL:<http://www.securityfocus.com/bid/48539>URL:<http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html>URL:<https://security.appspot.com/vsftpd.html>[\[return to 192.168.8.102 \]](#)**2.1.5 High 3632/tcp**

High (CVSS: 9.3)

NVT: DistCC Remote Code Execution Vulnerability

Summary

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

Vulnerability Detection Result

It was possible to execute the "id" command.

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

Solution**Solution type:** VendorFix

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

Vulnerability Detection Method

Details:DistCC Remote Code Execution Vulnerability

OID:1.3.6.1.4.1.25623.1.0.103553

Version used: \$Revision: 5120 \$

References

CVE: CVE-2004-2687

Other:

URL:<http://distcc.samba.org/security.html>URL:<http://archives.neohapsis.com/archives/bugtraq/2005-03/0183.html>

High (CVSS: 8.5) NVT: DistCC Detection
Summary DistCC is a program to distribute builds of C, C++, Objective C or Objective C++ code across several machines on a network. DistCC should always generate the same results as a local build, is simple to install and use, and is often two or more times faster than a local compile.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.
Solution Solution type: Mitigation For more information about DistCC's security see: http://distcc.samba.org/security.html
Vulnerability Detection Method Details:DistCC Detection OID:1.3.6.1.4.1.25623.1.0.12638 Version used: \$Revision: 5420 \$

[[return to 192.168.8.102](#)]

2.1.6 High 80/tcp

High (CVSS: 10.0) NVT: TWiki XSS and Command Execution Vulnerabilities
Product detection result cpe:/a:twiki:twiki:01.Feb.2003 Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
Summary The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 4.2.4
Impact Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application. ... continues on next page ...

...continued from previous page ...
Impact Level: Application
Solution Solution type: VendorFix Upgrade to version 4.2.4 or later, http://twiki.org/cgi-bin/view/Codev/TWikiRelease04x02x04
Affected Software/OS TWiki, TWiki version prior to 4.2.4.
Vulnerability Insight The flaws are due to, - %URLPARAM}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack. - %SEARCH}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.
Vulnerability Detection Method Details:TWiki XSS and Command Execution Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.800320 Version used: \$Revision: 4227 \$
Product Detection Result Product: cpe:/a:twiki:twiki:01.Feb.2003 Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)
References CVE: CVE-2008-5304, CVE-2008-5305 BID:32668, 32669 Other: URL: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304 URL: http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305

High (CVSS: 7.5)

NVT: phpinfo() output accessible

Summary

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

Vulnerability Detection Result

The following files are calling the function phpinfo() which disclose potentiall
↳y sensitive information to the remote attacker:

<http://192.168.8.102/phpinfo.php>

<http://192.168.8.102/mutillidae/phpinfo.php>

... continues on next page ...

...continued from previous page ...
Impact Some of the information that can be gathered from this file includes: The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, the system version(unix / linux), and the root directory of the web server.
Solution Solution type: Workaround Delete them or restrict access to the listened files.
Vulnerability Detection Method Details:phpinfo() output accessible OID:1.3.6.1.4.1.25623.1.0.11229 Version used: \$Revision: 5815 \$
High (CVSS: 7.5) NVT: phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary phpMyAdmin is prone to multiple input-validation vulnerabilities, including an HTTP response-splitting vulnerability and a local file-include vulnerability. These issues can be leveraged to view or execute arbitrary local scripts, or misrepresent how web content is served, cached, or interpreted. This could aid in various attacks that try to entice client users into a false sense of trust. Other attacks are also possible. Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.
Vulnerability Detection Method Details:phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100078 Version used: \$Revision: 5016 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
... continues on next page ...

...continued from previous page ...

References

BID:34253

Other:

URL:<http://www.securityfocus.com/bid/34253>

High (CVSS: 7.5)

NVT: phpMyAdmin Code Injection and XSS Vulnerability

Product detection result

cpe:/a:phpmyadmin:phpmyadmin:3.1.1

Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary

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

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

Versions prior to phpMyAdmin 2.11.9.5 and 3.1.3.1 are vulnerable.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

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

Vulnerability Detection Method

Details:phpMyAdmin Code Injection and XSS Vulnerability

OID:1.3.6.1.4.1.25623.1.0.100077

Version used: \$Revision: 5016 \$

Product Detection Result

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

Method: phpMyAdmin Detection

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

CVE: CVE-2009-1151

BID:34236, 34251

Other:

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

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

High (CVSS: 7.5) NVT: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities
Product detection result cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.↪0.901001)
Summary Tiki Wiki CMS Groupware is prone to multiple unspecified vulnerabilities, including: - An unspecified SQL-injection vulnerability - An unspecified authentication-bypass vulnerability - An unspecified vulnerability
Vulnerability Detection Result Installed version: 1.9.5 Fixed version: 4.2
Impact Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible.
Solution Solution type: VendorFix The vendor has released an advisory and fixes. Please see the references for details.
Affected Software/OS Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.
Vulnerability Detection Method Details:Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100537 Version used: \$Revision: 5144 \$
Product Detection Result Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Method: Tiki Wiki CMS Groupware Version Detection OID: 1.3.6.1.4.1.25623.1.0.901001)
References CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136 BID:38608 Other: URL:http://www.securityfocus.com/bid/38608 URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=247↪34
... continues on next page ...

...continued from previous page...
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=250 ↪46
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254 ↪24
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254 ↪35
URL:http://info.tikiwiki.org/article86-Tiki-Announces-3-5-and-4-2-Releases
URL:http://info.tikiwiki.org/tiki-index.php?page=homepage

High (CVSS: 7.5)

NVT: phpMyAdmin Configuration File PHP Code Injection Vulnerability

Product detection result

cpe:/a:phpmyadmin:phpmyadmin:3.1.1

Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary

According to its version number, the remote version of phpMyAdmin is prone to a remote PHP code-injection vulnerability.

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

phpMyAdmin 3.x versions prior to 3.1.3.2 are vulnerable.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

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

Vulnerability Detection Method

Details:phpMyAdmin Configuration File PHP Code Injection Vulnerability

OID:1.3.6.1.4.1.25623.1.0.100144

Version used: \$Revision: 5016 \$

Product Detection Result

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

Method: phpMyAdmin Detection

OID: 1.3.6.1.4.1.25623.1.0.900129)

References

CVE: CVE-2009-1285

BID:34526

Other:

URL:<http://www.securityfocus.com/bid/34526>

High (CVSS: 7.5) NVT: Test HTTP dangerous methods
Summary Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files.
Vulnerability Detection Result We could upload the following files via the PUT method at this web server: http://192.168.8.102/dav/puttest521514580.html We could delete the following files via the DELETE method at this web server: http://192.168.8.102/dav/puttest521514580.html
Impact - Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server. - Enabled DELETE method: This might allow an attacker to delete additional files on this web server.
Solution Solution type: Mitigation Use access restrictions to these dangerous HTTP methods or disable them completely.
Vulnerability Detection Method Details:Test HTTP dangerous methods OID:1.3.6.1.4.1.25623.1.0.10498 Version used: \$Revision: 4295 \$
References BID:12141 Other: OWASP:OWASP-CM-001

High (CVSS: 7.5) NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.
Summary PHP is prone to an information-disclosure vulnerability.
Vulnerability Detection Result Vulnerable url: http://192.168.8.102/cgi-bin/php
Impact Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer other attacks are also possible.
... continues on next page ...

...continued from previous page ...

Solution**Solution type:** VendorFix

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

Vulnerability Insight

When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.

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

`http://localhost/index.php?-s`

Vulnerability Detection Method

Details:PHP-CGI-based setups vulnerability when parsing query string parameters from ph.
↪..

OID:1.3.6.1.4.1.25623.1.0.103482

Version used: \$Revision: 5958 \$

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-risks-Update-1567532.html>

URL:<http://www.kb.cert.org/vuls/id/520827>

URL:<http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/>

URL:<https://bugs.php.net/bug.php?id=61910>

URL:<http://www.php.net/manual/en/security.cgi-bin.php>

URL:<http://www.securityfocus.com/bid/53388>

[\[return to 192.168.8.102 \]](#)

2.1.7 High 6200/tcp

High (CVSS: 7.5)

NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary

vsftpd is prone to a backdoor vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

...continued from previous page ...
Impact Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
Solution Solution type: VendorFix The repaired package can be downloaded from https://security.appspot.com/vsftpd.html . Please validate the package with its signature.
Affected Software/OS The vsftpd 2.3.4 source package is affected.
Vulnerability Detection Method Details:vsftpd Compromised Source Packages Backdoor Vulnerability OID:1.3.6.1.4.1.25623.1.0.103185 Version used: \$Revision: 5026 \$
References BID:48539 Other: URL: http://www.securityfocus.com/bid/48539 URL: http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html URL: https://security.appspot.com/vsftpd.html

[\[return to 192.168.8.102 \]](#)

2.1.8 High 5900/tcp

High (CVSS: 9.0) NVT: VNC Brute Force Login
Summary Try to log in with given passwords via VNC protocol.
Vulnerability Detection Result It was possible to connect to the VNC server with the password: password
Solution Solution type: Mitigation Change the password to something hard to guess.
Vulnerability Insight This script tries to authenticate to a VNC server with the passwords set in the password preference.
... continues on next page ...

...continued from previous page ...

Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked. Note as well that passwords can be max. 8 characters long.

Vulnerability Detection Method

Details:VNC Brute Force Login

OID:1.3.6.1.4.1.25623.1.0.106056

Version used: \$Revision: 4472 \$

[\[return to 192.168.8.102 \]](#)**2.1.9 High 1099/tcp**

High (CVSS: 10.0)

NVT: Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability

Summary

Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution**Solution type:** Workaround

Disable class-loading.

Vulnerability Insight

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

Vulnerability Detection Method

Check if the target tries to load a Java class via a remote HTTP URL.

Details:Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerabil.

↪..

OID:1.3.6.1.4.1.25623.1.0.140051

Version used: \$Revision: 4422 \$

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

[\[return to 192.168.8.102 \]](#)

2.1.10 High general/tcp

High (CVSS: 10.0) NVT: OS End Of Life Detection
Summary OS End Of Life Detection The Operating System on the remote host has reached the end of life and should not be used anymore
Vulnerability Detection Result The Operating System (cpe:/o:canonical:ubuntu_linux:8.04) on the remote host has ↩ reached the end of life at 09 May 2013 and should not be used anymore. See https://wiki.ubuntu.com/Releases for more information.
Vulnerability Detection Method Details:OS End Of Life Detection OID:1.3.6.1.4.1.25623.1.0.103674 Version used: \$Revision: 5464 \$

[\[return to 192.168.8.102 \]](#)

2.1.11 Medium 6667/tcp

Medium (CVSS: 6.8) NVT: UnrealIRCd Authentication Spoofing Vulnerability
Product detection result cpe:/a:unrealircd:unrealircd:3.2.8.1 Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)
Summary This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability.
Vulnerability Detection Result Installed version: 3.2.8.1 Fixed version: 3.2.10.7
Impact Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user. Impact Level: Application. ... continues on next page ...

...continued from previous page ...
Solution Solution type: VendorFix Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later. For updates refer to https://bugs.unrealircd.org/main_page.php
Affected Software/OS UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.
Vulnerability Insight The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.
Vulnerability Detection Method Get the installed version with the help of detect NVT and check the version is vulnerable or not. Details:UnrealIRCd Authentication Spoofing Vulnerability OID:1.3.6.1.4.1.25623.1.0.809883 Version used: \$Revision: 5287 \$
Product Detection Result Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection OID: 1.3.6.1.4.1.25623.1.0.809884)
References CVE: CVE-2016-7144 BID:92763 Other: URL: http://seclists.org/oss-sec/2016/q3/420 URL: http://www.openwall.com/lists/oss-security/2016/09/05/8 URL: https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf8c6bc50ba1a34a766

[\[return to 192.168.8.102 \]](#)

2.1.12 Medium 445/tcp

Medium (CVSS: 6.0) NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)
Product detection result cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
Summary ... continues on next page ...

...continued from previous page ...
Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.
Solution Solution type: VendorFix Updates are available. Please see the referenced vendor advisory.
Affected Software/OS This issue affects Samba 3.0.0 to 3.0.25rc3.
Vulnerability Detection Method Send a crafted command to the samba server and check for a remote command execution. Details:Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check) OID:1.3.6.1.4.1.25623.1.0.108011 Version used: \$Revision: 4401 \$
Product Detection Result Product: cpe:/a:samba:samba:3.0.20 Method: SMB NativeLanMan OID: 1.3.6.1.4.1.25623.1.0.102011)
References CVE: CVE-2007-2447 BID:23972 Other: URL:http://www.securityfocus.com/bid/23972 URL:https://www.samba.org/samba/security/CVE-2007-2447.html

[[return to 192.168.8.102](#)]

2.1.13 Medium 5432/tcp

Medium (CVSS: 6.8) NVT: PostgreSQL Multiple Security Vulnerabilities
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
... continues on next page ...

...continued from previous page ...
<p>Summary</p> <p>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.</p>
<p>Vulnerability Detection Result</p> <p>Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Solution</p> <p>Updates are available. Please see the references for more information.</p>
<p>Vulnerability Detection Method</p> <p>Details:PostgreSQL Multiple Security Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100273 Version used: \$Revision: 5016 \$</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)</p>
<p>References</p> <p>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</p>
<p>Medium (CVSS: 6.8) NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability</p>
<p>Summary</p> <p>OpenSSL is prone to security-bypass vulnerability.</p>
<p>Vulnerability Detection Result</p> <p>Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Impact</p> <p>... continues on next page ...</p>

...continued from previous page ...
Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.
Solution Solution type: VendorFix Updates are available.
Affected Software/OS OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h
Vulnerability Insight OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.
Vulnerability Detection Method Send two SSL ChangeCipherSpec request and check the response. Details:SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.105042 Version used: \$Revision: 5537 \$
References CVE: CVE-2014-0224 BID:67899 Other: URL:http://www.securityfocus.com/bid/67899 URL:http://openssl.org/
Medium (CVSS: 6.5) NVT: PostgreSQL '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.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
... continues on next page ...

...continued from previous page...
Solution Updates are available. Please see the references for more information.
Vulnerability Detection Method Details:PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.103054 Version used: \$Revision: 3911 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2010-4015 BID:46084 Other: URL: https://www.securityfocus.com/bid/46084 URL: http://www.postgresql.org/ URL: http://www.postgresql.org/about/news.1289

Medium (CVSS: 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.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Vulnerability Detection Method Details:PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.100470 Version used: \$Revision: 5394 \$
Product Detection Result ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2010-0442 BID:37973 Other: URL:http://www.postgresql.org/ URL:http://www.securityfocus.com/bid/37973 URL:http://xforce.iss.net/xforce/xfdb/55902 URL:http://intevydis.blogspot.com/2010/01/postgresql-8023-bitsubstr-overflow. ↪html

Medium (CVSS: 6.5) NVT: PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary PostgreSQL is prone to a security-bypass vulnerability because the application fails to properly validate the domain name in a signed CA certificate, allowing attackers to substitute malicious SSL certificates for trusted ones. 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.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution Updates are available. Please see the references for more information.
Vulnerability Detection Method Details:PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnera. ↪.. OID:1.3.6.1.4.1.25623.1.0.100400 Version used: \$Revision: 5016 \$
Product Detection Result
... continues on next page ...

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

Medium (CVSS: 6.0) NVT: PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary PostgreSQL is prone to a local privilege-escalation vulnerability. 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.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution Updates are available. Please see the references for more information.
Vulnerability Detection Method Details:PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability OID:1.3.6.1.4.1.25623.1.0.100843 Version used: \$Revision: 5373 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References ... continues on next page ...

...continued from previous page ...
<p>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</p>
<p>Medium (CVSS: 5.5) NVT: PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability</p>
<p>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)</p>
<p>Summary PostgreSQL is prone to an unauthorized-access vulnerability. Attackers can exploit this issue to reset special parameter settings only a root user should be able to modify. This may aid in further attacks. This issue affects versions prior to the following PostgreSQL versions: 7.4.29, 8.0.25 8.1.21, 8.2.17 8.3.11 8.4.4</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Solution Updates are available. Please see the references for more information.</p>
<p>Vulnerability Detection Method Details: PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability OID: 1.3.6.1.4.1.25623.1.0.100648 Version used: \$Revision: 5373 \$</p>
<p>Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)</p>
<p>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</p>
... continues on next page ...

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

Medium (CVSS: 5.0) NVT: SSL/TLS: Certificate Expired
Summary The remote server's SSL/TLS certificate has already expired.
Vulnerability Detection Result The certificate of the remote service expired on 2010-04-16 14:07:45. Certificate details: subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6 ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX subject alternative names (SAN): None issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6 ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX serial: 00FAF93A4C7FB6B9CC valid from : 2010-03-17 14:07:45 UTC valid until: 2010-04-16 14:07:45 UTC fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436 ↪DE813CC
Solution Solution type: Mitigation Replace the SSL/TLS certificate by a new one.
Vulnerability Insight This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.
Vulnerability Detection Method Details:SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: \$Revision: 4765 \$

Medium (CVSS: 4.3) NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
Summary This host is prone to an information disclosure vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application
Solution Solution type: Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
Vulnerability Insight The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
Vulnerability Detection Method Evaluate previous collected information about this service. Details:SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability . ↪.. OID:1.3.6.1.4.1.25623.1.0.802087 Version used: \$Revision: 4749 \$
References CVE: CVE-2014-3566 BID:70574 Other: URL:https://www.openssl.org/~bodo/ssl-poodle.pdf URL:https://www.imperialviolet.org/2014/10/14/poodle.html URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit- ↪ing-ssl-30.html
Medium (CVSS: 4.3) NVT: SSL/TLS: Report Weak Cipher Suites
Summary ... continues on next page ...

...continued from previous page ...
<p>This routine reports all Weak SSL/TLS cipher suites accepted by a service.</p> <p>NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.</p>
<p>Vulnerability Detection Result</p> <p>'Weak' cipher suites accepted by this service via the SSLv3 protocol: TLS_RSA_WITH_RC4_128_SHA</p> <p>'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_SHA</p>
<p>Solution</p> <p>Solution type: Mitigation</p> <p>The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.</p> <p>Please see the references for more resources supporting you with this task.</p>
<p>Vulnerability Insight</p> <p>These rules are applied for the evaluation of the cryptographic strength:</p> <ul style="list-style-type: none"> - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000). - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong
<p>Vulnerability Detection Method</p> <p>Details:SSL/TLS: Report Weak Cipher Suites</p> <p>OID:1.3.6.1.4.1.25623.1.0.103440</p> <p>Version used: \$Revision: 5525 \$</p>
<p>References</p> <p>CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000</p> <p>Other:</p> <p>URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html</p> <p>URL:https://bettercrypto.org/</p> <p>URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/</p>
<p>Medium (CVSS: 4.3)</p> <p>NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection</p>
<p>Summary</p> <p>It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.</p>
<p>Vulnerability Detection Result</p> <p>... continues on next page ...</p>

...continued from previous page ...
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT.
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Solution Solution type: Mitigation It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.
Affected Software/OS All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
Vulnerability Insight The SSLv2 and SSLv3 protocols containing known cryptographic flaws like: - Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566) - Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)
Vulnerability Detection Method Check the used protocols of the services provided by this system. Details:SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012 Version used: \$Revision: 5547 \$
References CVE: CVE-2016-0800, CVE-2014-3566 Other: URL: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report URL: https://bettercrypto.org/ URL: https://mozilla.github.io/server-side-tls/ssl-config-generator/ URL: https://drownattack.com/ URL: https://www.imperialviolet.org/2014/10/14/poodle.html
Medium (CVSS: 4.0) NVT: PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
... continues on next page ...

...continued from previous page ...
Summary PostgreSQL is prone to a remote denial-of-service vulnerability. Exploiting this issue may allow attackers to terminate connections to the PostgreSQL server, denying service to legitimate users.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution Updates are available. Update to newer Version.
Vulnerability Detection Method Details:PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.100157 Version used: \$Revision: 5016 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2009-0922 BID:34090 Other: URL: http://www.securityfocus.com/bid/34090 URL: http://www.postgresql.org/

Medium (CVSS: 4.0) NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
Summary The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
Vulnerability Detection Result Server Temporary Key Size: 1024 bits
Impact An attacker might be able to decrypt the SSL/TLS communication offline.
Solution Solution type: Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html)
... continues on next page ...

...continued from previous page ...
Vulnerability Insight The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.
Vulnerability Detection Method Checks the DHE temporary public key size. Details:SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili. ↪.. OID:1.3.6.1.4.1.25623.1.0.106223 Version used: \$Revision: 5825 \$
References Other: URL:https://weakdh.org/ URL:https://weakdh.org/sysadmin.html

Medium (CVSS: 4.0) NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
Summary The remote service is using a SSL/TLS certificate chain that has been signed using a cryptographically weak hashing algorithm.
Vulnerability Detection Result The following certificates are part of the certificate chain but using insecure ↪signature algorithms: Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173 ↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic ↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi ↪ng outside US,C=XX Signature Algorithm: sha1WithRSAEncryption
Solution Solution type: Mitigation Servers that use SSL/TLS certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL/TLS certificates to avoid these web browser SSL/TLS certificate warnings.
Vulnerability Insight Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not secure enough for ongoing use. Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when users visit web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
Vulnerability Detection Method ... continues on next page ...

...continued from previous page ...
Check which algorithm was used to sign the remote SSL/TLS Certificate. Details:SSL/TLS: Certificate Signed Using A Weak Signature Algorithm OID:1.3.6.1.4.1.25623.1.0.105880 Version used: \$Revision: 4781 \$
References Other: URL: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

[\[return to 192.168.8.102 \]](#)

2.1.14 Medium 21/tcp

Medium (CVSS: 6.4) NVT: Check for Anonymous FTP Login
Summary This FTP Server allows anonymous logins.
Vulnerability Detection Result It was possible to login to the remote FTP service with the following anonymous ↪account: anonymous:openvas@example.com ftp:openvas@example.com
Impact Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to: - gain access to sensitive files - upload or delete files
Solution Solution type: Mitigation If you do not want to share files, you should disable anonymous logins.
Vulnerability Insight A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.
Vulnerability Detection Method Try to login with an anonymous account at the remove FTP service. Details:Check for Anonymous FTP Login
... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.900600 Version used: \$Revision: 4987 \$
References Other: URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497

[\[return to 192.168.8.102 \]](#)

2.1.15 Medium 80/tcp

Medium (CVSS: 6.8) NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10
Product detection result cpe:/a:twiki:twiki:01.Feb.2003 Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
Summary The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.
Vulnerability Detection Result Installed version: 01.Feb.2003 Fixed version: 4.3.2
Impact Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack. Impact Level: Application
Solution Solution type: VendorFix Upgrade to TWiki version 4.3.2 or later, For updates refer to http://twiki.org/cgi-bin/view/Codev/DownloadTWiki
Affected Software/OS TWiki version prior to 4.3.2
Vulnerability Insight Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.
Vulnerability Detection Method Details:TWiki Cross-Site Request Forgery Vulnerability - Sep10 ... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.801281 Version used: \$Revision: 4293 \$
Product Detection Result Product: cpe:/a:twiki:twiki:01.Feb.2003 Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)
References CVE: CVE-2009-4898 Other: URL:http://www.openwall.com/lists/oss-security/2010/08/03/8 URL:http://www.openwall.com/lists/oss-security/2010/08/02/17 URL:http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix

Medium (CVSS: 6.5) NVT: phpMyAdmin Bookmark Security Bypass Vulnerability
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary phpMyAdmin is prone to a security-bypass vulnerability that affects bookmarks. Successfully exploiting this issue allows a remote attacker to bypass certain security restrictions and perform unauthorized actions. Versions prior to phpMyAdmin 3.3.9.2 and 2.11.11.3 are vulnerable.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution Updates are available. Please see the references for details.
Vulnerability Detection Method Details:phpMyAdmin Bookmark Security Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.103076 Version used: \$Revision: 3911 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
... continues on next page ...

...continued from previous page ...

References

CVE: CVE-2011-0987

BID: 46359

Other:

URL: <https://www.securityfocus.com/bid/46359>URL: <http://www.phpmyadmin.net/>URL: http://www.phpmyadmin.net/home_page/security/PMASA-2011-2.php

Medium (CVSS: 6.0)

NVT: TWiki Cross-Site Request Forgery Vulnerability

Product detection result

cpe:/a:twiki:twiki:01.Feb.2003

Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary

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

Vulnerability Detection Result

Installed version: 01.Feb.2003

Fixed version: 4.3.1

Impact

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

Impact Level: Application

Solution**Solution type:** VendorFixUpgrade to version 4.3.1 or later, <http://twiki.org/cgi-bin/view/Codev/DownloadTWiki>**Affected Software/OS**

TWiki version prior to 4.3.1

Vulnerability Insight

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

Vulnerability Detection Method

Details: TWiki Cross-Site Request Forgery Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.800400

Version used: \$Revision: 4892 \$

Product Detection Result

... continues on next page ...

...continued from previous page ...
Product: cpe:/a:twiki:twiki:01.Feb.2003 Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)
References CVE: CVE-2009-1339 Other: URL: http://secunia.com/advisories/34880 URL: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258 URL: http://twiki.org/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di ↪ff-cve-2009-1339.txt

Medium (CVSS: 5.8) NVT: http TRACE XSS attack
Summary Debugging functions are enabled on the remote HTTP server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.
Vulnerability Detection Result Solution: Add the following lines for each virtual host in your configuration file : <pre> RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE TRACK) RewriteRule .* - [F] </pre> See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
Solution Disable these methods.
Vulnerability Detection Method Details:http TRACE XSS attack OID:1.3.6.1.4.1.25623.1.0.11213 Version used: \$Revision: 3362 \$
References CVE: CVE-2004-2320, CVE-2003-1567 BID:9506, 9561, 11604 Other: URL: http://www.kb.cert.org/vuls/id/867593

Medium (CVSS: 5.0) NVT: /doc directory browsable
Summary The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.
Vulnerability Detection Result Vulnerable url: http://192.168.8.102/doc/
Solution Solution type: Mitigation Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf: <Directory /usr/doc> AllowOverride None order deny,allow deny from all allow from localhost </Directory>
Vulnerability Detection Method Details: /doc directory browsable OID: 1.3.6.1.4.1.25623.1.0.10056 Version used: \$Revision: 4288 \$
References CVE: CVE-1999-0678 BID: 318

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

...continued from previous page ...
Solution Solution type: VendorFix Upgrade to version 2.2 or latest http://info.tikiwiki.org/tiki-index.php?page=Get+Tiki&bl
Affected Software/OS Tiki Wiki CMS Groupware version prior to 2.2 on all running platform
Vulnerability Insight The vulnerability is due to input validation error in tiki-error.php which fails to sanitise before being returned to the user.
Vulnerability Detection Method Details:Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability OID:1.3.6.1.4.1.25623.1.0.800315 Version used: \$Revision: 5144 \$
Product Detection Result Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Method: Tiki Wiki CMS Groupware Version Detection OID: 1.3.6.1.4.1.25623.1.0.901001)
References CVE: CVE-2008-5318, CVE-2008-5319 Other: URL: http://secunia.com/advisories/32341 URL: http://info.tikiwiki.org/tiki-read_article.php?articleId=41

Medium (CVSS: 5.0) NVT: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability
Product detection result cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)
Summary The host is installed with Tiki Wiki CMS Groupware and is prone to a local file inclusion vulnerability.
Vulnerability Detection Result Installed version: 1.9.5 Fixed version: 2.2.11
Impact ... continues on next page ...

...continued from previous page ...
<p>Successful exploitation will allow an user having access to the admin backend to gain access to arbitrary files and to compromise the application.</p> <p>Impact Level: System/Application</p>
<p>Solution</p> <p>Solution type: VendorFix</p> <p>Upgrade to Tiki Wiki CMS Groupware version 12.11 LTS, 15.4 or later. For updates refer to https://tiki.org</p>
<p>Affected Software/OS</p> <p>Tiki Wiki CMS Groupware versions:</p> <ul style="list-style-type: none"> - below 12.11 LTS - 13.x, 14.x and 15.x below 15.4
<p>Vulnerability Insight</p> <p>The Flaw is due to improper sanitization of input passed to the 'fixedURLData' parameter of the 'display_banner.php' script.</p>
<p>Vulnerability Detection Method</p> <p>Get the installed version with the help of the detect NVT and check the version is vulnerable or not.</p> <p>Details:Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability OID:1.3.6.1.4.1.25623.1.0.108064 Version used: \$Revision: 5144 \$</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 Method: Tiki Wiki CMS Groupware Version Detection OID: 1.3.6.1.4.1.25623.1.0.901001)</p>
<p>References</p> <p>CVE: CVE-2016-10143</p> <p>Other:</p> <p>URL:http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-released</p> <p>URL:https://sourceforge.net/p/tikiwiki/code/60308/</p>
<p>Medium (CVSS: 5.0)</p> <p>NVT: awiki Multiple Local File Include Vulnerabilities</p>
<p>Summary</p> <p>awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.</p>
<p>Vulnerability Detection Result</p>
... continues on next page ...

...continued from previous page ...
Vulnerable url: http://192.168.8.102/mutillidae/index.php?page=/etc/passwd
Impact An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host other attacks are also possible.
Solution Solution type: WillNotFix No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
Affected Software/OS awiki 20100125 is vulnerable other versions may also be affected.
Vulnerability Detection Method Details:awiki Multiple Local File Include Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.103210 Version used: \$Revision: 5651 \$
References BID:49187 Other: URL: http://www.securityfocus.com/bid/49187 URL: http://www.kobaonline.com/awiki/
Medium (CVSS: 4.3) NVT: phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary phpMyAdmin is prone to SQL-injection and cross-site scripting vulnerabilities because it fails to sufficiently sanitize user- supplied data. Exploiting these issues could allow an attacker to steal cookie- based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. Versions prior to phpMyAdmin 2.11.9.6 and 3.2.2.1 are affected.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
... continues on next page ...

...continued from previous page...	
Solution	Vendor updates are available. Please see the references for details.
Vulnerability Detection Method	Details:phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100307 Version used: \$Revision: 5016 \$
Product Detection Result	Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References	CVE: CVE-2009-3696 BID:36658 Other: URL:http://www.securityfocus.com/bid/36658 URL:http://www.phpmyadmin.net/ URL:http://freshmeat.net/projects/phpmyadmin/releases/306669 URL:http://freshmeat.net/projects/phpmyadmin/releases/306667

Medium (CVSS: 4.3) NVT: phpMyAdmin Database Search Cross Site Scripting Vulnerability	
Product detection result	cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary	phpMyAdmin is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks. Versions prior to phpMyAdmin 3.3.8.1 and 2.11.11.1 are vulnerable.
Vulnerability Detection Result	Vulnerability was detected according to the Vulnerability Detection Method.
Solution	Vendor updates are available. Please see the references for more information.
Vulnerability Detection Method	Details:phpMyAdmin Database Search Cross Site Scripting Vulnerability
... continues on next page ...	

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.100939 Version used: \$Revision: 5323 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References CVE: CVE-2010-4329 BID:45100 Other: URL:https://www.securityfocus.com/bid/45100 URL:http://www.phpmyadmin.net/ URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-8.php

Medium (CVSS: 4.3) NVT: phpMyAdmin SQL bookmark XSS Vulnerability
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary This host is running phpMyAdmin and is prone to Cross Site Scripting vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will let the attacker cause XSS attacks and inject malicious web script or HTML code via a crafted SQL bookmarks.
Solution Apply the respective patches or upgrade to version 3.2.0.1 http://www.phpmyadmin.net/home_page/downloads.php http://phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin/ *** Note: Ignore the warning if above mentioned patches are applied. *****
Affected Software/OS phpMyAdmin version 3.0.x to 3.2.0.rc1
Vulnerability Insight This flaw arises because the input passed into SQL bookmarks is not adequately sanitised before using it in dynamically generated content.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Details:phpMyAdmin SQL bookmark XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.800595 Version used: \$Revision: 4869 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References CVE: CVE-2009-2284 BID:35543 Other: URL:http://secunia.com/advisories/35649 URL:http://www.phpmyadmin.net/home_page/security/PMASA-2009-5.php

Medium (CVSS: 4.3) NVT: phpMyAdmin Multiple Cross Site Scripting Vulnerabilities
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary phpMyAdmin is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input. An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. The following versions are vulnerable: phpMyAdmin 2.11.x prior to 2.11.10.1 phpMyAdmin 3.x prior to 3.3.5.1
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Solution Updates are available. Please see the references for details.
Vulnerability Detection Method Details:phpMyAdmin Multiple Cross Site Scripting Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100761 Version used: \$Revision: 5323 \$
...continues on next page ...

...continued from previous page ...

Product Detection Result

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

References

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

Medium (CVSS: 4.3)

NVT: phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability

Product detection result

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

Summary

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

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

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

Vulnerability Detection Method

Details: phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability
 OID: 1.3.6.1.4.1.25623.1.0.100775
 Version used: \$Revision: 5323 \$

Product Detection Result

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

... continues on next page ...

...continued from previous page ...
References CVE: CVE-2010-2958 BID: 42874 Other: URL: https://www.securityfocus.com/bid/42874 URL: http://www.phpmyadmin.net/ URL: http://www.phpmyadmin.net/home_page/security/PMASA-2010-6.php URL: http://www.phpmyadmin.git.sourceforge.net/git/gitweb.cgi?p=phpmyadmin/phpmyadmin;a=commitdiff;h=133a77fac7d31a38703db2099a90c1b49de62e37
Medium (CVSS: 4.3) NVT: phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow attackers to execute arbitrary web script or HTML in a user's browser session in the context of an affected site. Impact Level: Application
Solution Upgrade to phpMyAdmin version 3.3.7 or later, For updates refer to http://www.phpmyadmin.net/home_page/downloads.php
Affected Software/OS phpMyAdmin versions 3.x before 3.3.7
Vulnerability Insight The flaw is caused by an unspecified input validation error when processing spoofed requests sent to setup script, which could be exploited by attackers to cause arbitrary scripting code to be executed on the user's browser session in the security context of an affected site.
Vulnerability Detection Method Details: phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability OID: 1.3.6.1.4.1.25623.1.0.801286 Version used: \$Revision: 5373 \$
... continues on next page ...

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

Medium (CVSS: 4.3) NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
Product detection result cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Summary The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks. Impact Level: Application
Solution Solution type: WillNotFix No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
Affected Software/OS phpMyAdmin version 3.3.8.1 and prior.
Vulnerability Insight The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Method Details:phpMyAdmin 'error.php' Cross Site Scripting Vulnerability OID:1.3.6.1.4.1.25623.1.0.801660 Version used: \$Revision: 5323 \$
Product Detection Result Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
References CVE: CVE-2010-4480 Other: URL:http://www.exploit-db.com/exploits/15699/ URL:http://www.vupen.com/english/advisories/2010/3133

Medium (CVSS: 4.3) NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
Summary This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks. Impact Level: Application
Solution Solution type: VendorFix Upgrade to Apache HTTP Server version 2.2.22 or later, For updates refer to http://httpd.apache.org/
Affected Software/OS Apache HTTP Server versions 2.2.0 through 2.2.21
Vulnerability Insight The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.
Vulnerability Detection Method Details:Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability ... continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.902830 Version used: \$Revision: 5950 \$
References CVE: CVE-2012-0053 BID:51706 Other: URL:http://secunia.com/advisories/47779 URL:http://www.exploit-db.com/exploits/18442 URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html URL:http://httpd.apache.org/security/vulnerabilities_22.html URL:http://svn.apache.org/viewvc?view=revision&revision=1235454 URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm ↪1

[[return to 192.168.8.102](#)]

2.1.16 Medium 22/tcp

Medium (CVSS: 4.3) NVT: SSH Weak Encryption Algorithms Supported
Summary The remote SSH server is configured to allow weak encryption algorithms.
Vulnerability Detection Result The following weak client-to-server encryption algorithms are supported by the remote service: 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se The following weak server-to-client encryption algorithms are supported by the remote service: 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128
... continues on next page ...

...continued from previous page ...
<pre>arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se</pre>
Solution Solution type: Mitigation Disable the weak encryption algorithms.
Vulnerability Insight The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore. The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.
Vulnerability Detection Method Check if remote ssh service supports Arcfour, none or CBC ciphers. Details:SSH Weak Encryption Algorithms Supported OID:1.3.6.1.4.1.25623.1.0.105611 Version used: \$Revision: 4490 \$
References Other: URL: https://tools.ietf.org/html/rfc4253#section-6.3 URL: https://www.kb.cert.org/vuls/id/958563

[[return to 192.168.8.102](#)]

2.1.17 Low 5432/tcp

Low (CVSS: 3.5) NVT: PostgreSQL Hash Table Integer Overflow Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary The host is running PostgreSQL and is prone to integer overflow vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
... continues on next page ...

...continued from previous page ...
Impact Successful exploitation could allow execution of specially-crafted sql query which once processed would lead to denial of service (postgresql daemon crash). Impact Level: Application
Solution Apply the patch, http://git.postgresql.org/gitweb?p=postgresql.git;a=commitdiff;h=64b057e6823655fb6c5d1f24a28f236b94dd6c54 **** NOTE: Please ignore this warning if the patch is applied. ****
Affected Software/OS PostgreSQL version 8.4.1 and prior and 8.5 through 8.5alpha2
Vulnerability Insight The flaw is due to an integer overflow error in 'src/backend/executor/nodeHash.c', when used to calculate size for the hashtable for joined relations.
Vulnerability Detection Method Details:PostgreSQL Hash Table Integer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.902139 Version used: \$Revision: 5401 \$
Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
References CVE: CVE-2010-0733 Other: URL: https://bugzilla.redhat.com/show_bug.cgi?id=546621 URL: http://www.openwall.com/lists/oss-security/2010/03/16/10 URL: http://archives.postgresql.org/pgsql-bugs/2009-10/msg00310.php URL: http://archives.postgresql.org/pgsql-bugs/2009-10/msg00289.php URL: http://archives.postgresql.org/pgsql-bugs/2009-10/msg00287.php URL: http://archives.postgresql.org/pgsql-bugs/2009-10/msg00277.php
Low (CVSS: 2.1) NVT: PostgreSQL Low Cost Function Information Disclosure Vulnerability
Product detection result cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Summary ... continues on next page ...

...continued from previous page ...
<p>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.</p>
<p>Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p>Vulnerability Detection Method Details:PostgreSQL Low Cost Function Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.100158 Version used: \$Revision: 5016 \$</p>
<p>Product Detection Result Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)</p>
<p>References BID:34069 Other: URL:http://www.securityfocus.com/bid/34069 URL:http://www.postgresql.org/</p>

[[return to 192.168.8.102](#)]

2.1.18 Low 22/tcp

<p>Low (CVSS: 2.6) NVT: SSH Weak MAC Algorithms Supported</p>
<p>Summary The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.</p>
<p>Vulnerability Detection Result The following weak client-to-server MAC algorithms are supported by the remote s ↪ervice: hmac-md5 hmac-md5-96 hmac-sha1-96 The following weak server-to-client MAC algorithms are supported by the remote s ↪ervice: hmac-md5 hmac-md5-96 hmac-sha1-96</p>
... continues on next page ...

...continued from previous page ...

Solution**Solution type:** Mitigation

Disable the weak MAC algorithms.

Vulnerability Detection Method

Details:SSH Weak MAC Algorithms Supported

OID:1.3.6.1.4.1.25623.1.0.105610

Version used: \$Revision: 4490 \$

[\[return to 192.168.8.102 \]](#)**2.1.19 Low general/tcp**

Low (CVSS: 2.6)

NVT: TCP timestamps

Summary

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

Vulnerability Detection Result

It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 2889476

Packet 2: 2889572

Impact

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

Solution**Solution type:** Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See also: <http://www.microsoft.com/en-us/download/details.aspx?id=9152>**Affected Software/OS**

TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight

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

... continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details:TCP timestamps

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: \$Revision: 5740 \$

References

Other:

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

[[return to 192.168.8.102](#)]

This file was automatically generated.