

# Scan Report

October 9, 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 “Metasploitable (Full and Fast)”. The scan started at Mon Oct 9 00:37:57 2017 UTC and ended at Mon Oct 9 00:56:05 2017 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

<b>1</b>	<b>Result Overview</b>	<b>2</b>
1.1	Host Authentications . . . . .	2
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	192.168.56.101 . . . . .	2
2.1.1	High 21/tcp . . . . .	3
2.1.2	High 512/tcp . . . . .	4
2.1.3	High 1524/tcp . . . . .	4
2.1.4	High 80/tcp . . . . .	5
2.1.5	High 1099/tcp . . . . .	11
2.1.6	High 5900/tcp . . . . .	12
2.1.7	High 8787/tcp . . . . .	12
2.1.8	High 6200/tcp . . . . .	14
2.1.9	High 22/tcp . . . . .	15
2.1.10	High 5432/tcp . . . . .	15
2.1.11	High 3306/tcp . . . . .	17
2.1.12	High 3632/tcp . . . . .	17
2.1.13	Medium 21/tcp . . . . .	18
2.1.14	Medium 80/tcp . . . . .	19
2.1.15	Medium 25/tcp . . . . .	31
2.1.16	Medium 445/tcp . . . . .	40
2.1.17	Medium 22/tcp . . . . .	41

2.1.18	Medium 5432/tcp . . . . .	42
2.1.19	Low general/tcp . . . . .	55
2.1.20	Low 22/tcp . . . . .	56
2.1.21	Low 5432/tcp . . . . .	57

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.56.101	20	39	4	0	0
Total: 1	20	39	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 63 results selected by the filtering described above. Before filtering there were 326 results.

### 1.1 Host Authentications

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

## 2 Results per Host

### 2.1 192.168.56.101

Host scan start Mon Oct 9 00:38:06 2017 UTC

Host scan end Mon Oct 9 00:56:05 2017 UTC

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

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
3306/tcp	High
3632/tcp	High
21/tcp	Medium
80/tcp	Medium
25/tcp	Medium
445/tcp	Medium
22/tcp	Medium
5432/tcp	Medium
general/tcp	Low
22/tcp	Low
5432/tcp	Low

**2.1.1 High 21/tcp**

<b>High (CVSS: 7.5)</b> <b>NVT: vsftpd Compromised Source Packages Backdoor Vulnerability</b>
<b>Summary</b> vsftpd is prone to a backdoor vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
<b>Solution</b> <b>Solution type:</b> VendorFix The repaired package can be downloaded from <a href="https://security.appspot.com/vsftpd.html">https://security.appspot.com/vsftpd.html</a> . Please validate the package with its signature.
<b>Affected Software/OS</b> The vsftpd 2.3.4 source package is affected.
<b>Vulnerability Detection Method</b> Details:vsftpd Compromised Source Packages Backdoor Vulnerability OID:1.3.6.1.4.1.25623.1.0.103185 Version used: \$Revision: 5026 \$
<b>References</b> BID:48539 Other: URL: <a href="http://www.securityfocus.com/bid/48539">http://www.securityfocus.com/bid/48539</a> URL: <a href="http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back">http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back</a>
... continues on next page ...

...continued from previous page ...

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

[ [return to 192.168.56.101](#) ]**2.1.2 High 512/tcp**

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

**Summary**

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

**Vulnerability Detection Result**

The rexecd Service is not allowing connections from this host.

**Solution**

**Solution type:** Mitigation  
 Disable rexec Service.

**Vulnerability Detection Method**

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

**References**

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

[ [return to 192.168.56.101](#) ]**2.1.3 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.

... continues on next page ...

...continued from previous page ...
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.
<b>Solution</b> <b>Solution type:</b> Workaround
<b>Vulnerability Detection Method</b> Details:Possible Backdoor: Ingreslock OID:1.3.6.1.4.1.25623.1.0.103549 Version used: \$Revision: 4718 \$

[ [return to 192.168.56.101](#) ]

#### 2.1.4 High 80/tcp

High (CVSS: 10.0) NVT: TWiki XSS and Command Execution Vulnerabilities
<b>Product detection result</b> cpe:/a:twiki:twiki:01.Feb.2003 Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
<b>Summary</b> The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.
<b>Vulnerability Detection Result</b> Installed version: 01.Feb.2003 Fixed version: 4.2.4
<b>Impact</b> Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application. Impact Level: Application
<b>Solution</b> <b>Solution type:</b> VendorFix Upgrade to version 4.2.4 or later, <a href="http://twiki.org/cgi-bin/view/Codev/TWikiRelease04x02x04">http://twiki.org/cgi-bin/view/Codev/TWikiRelease04x02x04</a>
<b>Affected Software/OS</b> TWiki, TWiki version prior to 4.2.4.
<b>Vulnerability Insight</b> ... continues on next page ...

...continued from previous page ...
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.
<b>Vulnerability Detection Method</b> Details:TWiki XSS and Command Execution Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.800320 Version used: \$Revision: 4227 \$
<b>Product Detection Result</b> Product: cpe:/a:twiki:twiki:01.Feb.2003 Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)
<b>References</b> 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://192.168.56.101/phpinfo.php

http://192.168.56.101/mutillidae/phpinfo.php

**Impact**

Some of the information that can be gathered from this file includes:

The username of the user who installed php, if they are a SUDO user, the IP 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.

... continues on next page ...

...continued from previous page...

**Vulnerability Detection Method**

Details:phpinfo() output accessible

OID:1.3.6.1.4.1.25623.1.0.11229

Version used: \$Revision: 6355 \$

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)

**References**

BID:34253

Other:

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



<p>High (CVSS: 7.5) NVT: phpMyAdmin Code Injection and XSS Vulnerability</p>
<p><b>Product detection result</b> cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p><b>Summary</b> 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.</p>
<p><b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p><b>Solution</b> Vendor updates are available. Please see <a href="http://www.phpmyadmin.net">http://www.phpmyadmin.net</a> for more Information.</p>
<p><b>Vulnerability Detection Method</b> Details:phpMyAdmin Code Injection and XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.100077 Version used: \$Revision: 5016 \$</p>
<p><b>Product Detection Result</b> Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p><b>References</b> CVE: CVE-2009-1151 BID:34236, 34251 Other: URL:<a href="http://www.securityfocus.com/bid/34236">http://www.securityfocus.com/bid/34236</a> URL:<a href="http://www.securityfocus.com/bid/34251">http://www.securityfocus.com/bid/34251</a></p>

<p>High (CVSS: 7.5) NVT: phpMyAdmin Configuration File PHP Code Injection Vulnerability</p>
<p><b>Product detection result</b> cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p>... continues on next page ...</p>

...continued from previous page ...
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Solution</b> Vendor updates are available. Please see <a href="http://www.phpmyadmin.net">http://www.phpmyadmin.net</a> for more Information.
<b>Vulnerability Detection Method</b> Details:phpMyAdmin Configuration File PHP Code Injection Vulnerability OID:1.3.6.1.4.1.25623.1.0.100144 Version used: \$Revision: 5016 \$
<b>Product Detection Result</b> Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
<b>References</b> CVE: CVE-2009-1285 BID:34526 Other: URL: <a href="http://www.securityfocus.com/bid/34526">http://www.securityfocus.com/bid/34526</a>

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

<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> We could upload the following files via the PUT method at this web server: <a href="http://192.168.56.101/dav/puttest1956436800.html">http://192.168.56.101/dav/puttest1956436800.html</a> We could delete the following files via the DELETE method at this web server: <a href="http://192.168.56.101/dav/puttest1956436800.html">http://192.168.56.101/dav/puttest1956436800.html</a>
<b>Impact</b> ... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> <li>- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.</li> <li>- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.</li> </ul>
<b>Solution</b> <b>Solution type:</b> Mitigation Use access restrictions to these dangerous HTTP methods or disable them completely.
<b>Vulnerability Detection Method</b> Details: Test HTTP dangerous methods OID: 1.3.6.1.4.1.25623.1.0.10498 Version used: \$Revision: 4295 \$
<b>References</b> 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.
<b>Summary</b> PHP is prone to an information-disclosure vulnerability.
<b>Vulnerability Detection Result</b> Vulnerable url: <a href="http://192.168.56.101/cgi-bin/php">http://192.168.56.101/cgi-bin/php</a>
<b>Impact</b> 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.
<b>Solution</b> <b>Solution type:</b> 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.
<b>Vulnerability Insight</b> 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: <a href="http://localhost/index.php?-s">http://localhost/index.php?-s</a>
... continues on next page ...

...continued from previous page ...
<b>Vulnerability Detection Method</b> 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 \$
<b>References</b> 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 192.168.56.101](#) ]

### 2.1.5 High 1099/tcp

High (CVSS: 10.0) NVT: Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Solution</b> <b>Solution type:</b> Workaround Disable class-loading.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> ... continues on next page ...

...continued from previous page ...
<p>Check if the target tries to load a Java class via a remote HTTP URL.</p> <p>Details:Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerabil.  ↔..</p> <p>OID:1.3.6.1.4.1.25623.1.0.140051</p> <p>Version used: \$Revision: 4422 \$</p>
<p><b>References</b></p> <p>Other:</p> <p>URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=23665</p>

[\[ return to 192.168.56.101 \]](#)

### 2.1.6 High 5900/tcp

<p>High (CVSS: 9.0)</p> <p>NVT: VNC Brute Force Login</p>
<p><b>Summary</b></p> <p>Try to log in with given passwords via VNC protocol.</p>
<p><b>Vulnerability Detection Result</b></p> <p>It was possible to connect to the VNC server with the password: password</p>
<p><b>Solution</b></p> <p><b>Solution type:</b> Mitigation</p> <p>Change the password to something hard to guess.</p>
<p><b>Vulnerability Insight</b></p> <p>This script tries to authenticate to a VNC server with the passwords set in the password preference.</p> <p>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.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Details:VNC Brute Force Login</p> <p>OID:1.3.6.1.4.1.25623.1.0.106056</p> <p>Version used: \$Revision: 4472 \$</p>

[\[ return to 192.168.56.101 \]](#)

### 2.1.7 High 8787/tcp

High (CVSS: 10.0) NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities
<p><b>Summary</b></p> <p>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>
<p><b>Vulnerability Detection Result</b></p> <p>The service is running in \$SAFE &gt;= 1 mode. However it is still possible to run a ↵rbbitrary 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><b>Impact</b></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><b>Solution</b></p> <p><b>Solution type:</b> 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"> <li>- Implementing taint on untrusted input</li> <li>- Setting \$SAFE levels appropriately (&gt;=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and &gt;=3 may be appropriate)</li> <li>- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts</li> </ul>
<p><b>Vulnerability Detection Method</b></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><b>References</b></p> <p>... continues on next page ...</p>

...continued from previous page ...
BID:47071 Other: URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=22750 URL:http://www.securityfocus.com/bid/47071 URL:http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_t ↪esters/ URL:http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html

[ [return to 192.168.56.101](#) ]

### 2.1.8 High 6200/tcp

<b>High (CVSS: 7.5)</b> <b>NVT: vsftpd Compromised Source Packages Backdoor Vulnerability</b>
<b>Summary</b> vsftpd is prone to a backdoor vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
<b>Solution</b> <b>Solution type:</b> VendorFix The repaired package can be downloaded from <a href="https://security.appspot.com/vsftpd.html">https://security.appspot.com/vsftpd.html</a> . Please validate the package with its signature.
<b>Affected Software/OS</b> The vsftpd 2.3.4 source package is affected.
<b>Vulnerability Detection Method</b> Details:vsftpd Compromised Source Packages Backdoor Vulnerability OID:1.3.6.1.4.1.25623.1.0.103185 Version used: \$Revision: 5026 \$
<b>References</b> BID:48539 Other: URL:http://www.securityfocus.com/bid/48539 URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back ↪doored.html URL:https://security.appspot.com/vsftpd.html

[\[ return to 192.168.56.101 \]](#)

### 2.1.9 High 22/tcp

High (CVSS: 9.0) NVT: SSH Brute Force Logins With Default Credentials Reporting
<p><b>Summary</b></p> <p>It was possible to login into the remote SSH server using default credentials. As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.</p>
<p><b>Vulnerability Detection Result</b></p> <p>It was possible to login with the following credentials &lt;User&gt;:&lt;Password&gt; msfadmin:msfadmin user:user</p>
<p><b>Solution</b></p> <p><b>Solution type:</b> Mitigation Change the password as soon as possible.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Try to login with a number of known default credentials via the SSH protocol. Details:SSH Brute Force Logins With Default Credentials Reporting OID:1.3.6.1.4.1.25623.1.0.103239 Version used: \$Revision: 5467 \$</p>

[\[ return to 192.168.56.101 \]](#)

### 2.1.10 High 5432/tcp

High (CVSS: 9.0) NVT: PostgreSQL weak password
<p><b>Summary</b></p> <p>It was possible to login into the remote PostgreSQL as user postgres using weak credentials.</p>
<p><b>Vulnerability Detection Result</b></p> <p>It was possible to login as user postgres with password "postgres".</p>
<p><b>Solution</b></p> <p>Change the password as soon as possible.</p>
<p><b>Vulnerability Detection Method</b></p> <p>... continues on next page ...</p>



...continued from previous page ...

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

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 192.168.56.101](#) ]

**2.1.11 High 3306/tcp**

High (CVSS: 9.0) NVT: MySQL / MariaDB weak password
<b>Summary</b> It was possible to login into the remote MySQL as root using weak credentials.
<b>Vulnerability Detection Result</b> It was possible to login as root with an empty password.
<b>Solution</b> <b>Solution type:</b> Mitigation Change the password as soon as possible.
<b>Vulnerability Detection Method</b> Details:MySQL / MariaDB weak password OID:1.3.6.1.4.1.25623.1.0.103551 Version used: \$Revision: 5889 \$

[\[ return to 192.168.56.101 \]](#)

**2.1.12 High 3632/tcp**

High (CVSS: 9.3) NVT: DistCC Remote Code Execution Vulnerability
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> It was possible to execute the "id" command. Result: uid=1(daemon) gid=1(daemon)
<b>Solution</b> <b>Solution type:</b> VendorFix Vendor updates are available. Please see the references for more information.
<b>Vulnerability Detection Method</b> Details:DistCC Remote Code Execution Vulnerability OID:1.3.6.1.4.1.25623.1.0.103553 Version used: \$Revision: 5120 \$
<b>References</b> ... continues on next page ...

...continued from previous page ...

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 192.168.56.101](#) ]**2.1.13 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

... continues on next page ...

...continued from previous page ...
<b>Impact</b> Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to: <ul style="list-style-type: none"> <li>- gain access to sensitive files</li> <li>- upload or delete files</li> </ul>
<b>Solution</b> <b>Solution type:</b> Mitigation If you do not want to share files, you should disable anonymous logins.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Try to login with an anonymous account at the remove FTP service. Details: Check for Anonymous FTP Login OID: 1.3.6.1.4.1.25623.1.0.900600 Version used: \$Revision: 4987 \$
<b>References</b> Other: URL: <a href="https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497">https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497</a>

[ [return to 192.168.56.101](#) ]

#### 2.1.14 Medium 80/tcp

Medium (CVSS: 6.8) NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10
<b>Product detection result</b> cpe:/a:twiki:twiki:01.Feb.2003 Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)
<b>Summary</b> The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.
<b>Vulnerability Detection Result</b> Installed version: 01.Feb.2003 Fixed version: 4.3.2
... continues on next page ...

...continued from previous page ...
<b>Impact</b> Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack. Impact Level: Application
<b>Solution</b> <b>Solution type:</b> VendorFix Upgrade to TWiki version 4.3.2 or later, For updates refer to <a href="http://twiki.org/cgi-bin/view/Codev/DownloadTWiki">http://twiki.org/cgi-bin/view/Codev/DownloadTWiki</a>
<b>Affected Software/OS</b> TWiki version prior to 4.3.2
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Details:TWiki Cross-Site Request Forgery Vulnerability - Sep10 OID:1.3.6.1.4.1.25623.1.0.801281 Version used: \$Revision: 4293 \$
<b>Product Detection Result</b> Product: cpe:/a:twiki:twiki:01.Feb.2003 Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)
<b>References</b> CVE: CVE-2009-4898 Other: URL: <a href="http://www.openwall.com/lists/oss-security/2010/08/03/8">http://www.openwall.com/lists/oss-security/2010/08/03/8</a> URL: <a href="http://www.openwall.com/lists/oss-security/2010/08/02/17">http://www.openwall.com/lists/oss-security/2010/08/02/17</a> URL: <a href="http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix">http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix</a>

Medium (CVSS: 6.5) NVT: phpMyAdmin Bookmark Security Bypass Vulnerability
<b>Product detection result</b> cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
<b>Summary</b> phpMyAdmin is prone to a security-bypass vulnerability that affects bookmarks.
... continues on next page ...

...continued from previous page ...
<p>Successfully exploiting this issue allows a remote attacker to bypass certain security restrictions and perform unauthorized actions.</p> <p>Versions prior to phpMyAdmin 3.3.9.2 and 2.11.11.3 are vulnerable.</p>
<p><b>Vulnerability Detection Result</b></p> <p>Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p><b>Solution</b></p> <p>Updates are available. Please see the references for details.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Details:phpMyAdmin Bookmark Security Bypass Vulnerability  OID:1.3.6.1.4.1.25623.1.0.103076  Version used: \$Revision: 3911 \$</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1  Method: phpMyAdmin Detection  OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p><b>References</b></p> <p>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</p>

<p>Medium (CVSS: 6.0)</p> <p>NVT: TWiki Cross-Site Request Forgery Vulnerability</p>
<p><b>Product detection result</b></p> <p>cpe:/a:twiki:twiki:01.Feb.2003  Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)</p>
<p><b>Summary</b></p> <p>The host is running TWiki and is prone to Cross-Site Request Forgery Vulnerability.</p>
<p><b>Vulnerability Detection Result</b></p> <p>Installed version: 01.Feb.2003  Fixed version: 4.3.1</p>
<p><b>Impact</b></p> <p>Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.</p>
... continues on next page ...

...continued from previous page ...	
Impact Level: Application	
<b>Solution</b> <b>Solution type:</b> VendorFix Upgrade to version 4.3.1 or later, <a href="http://twiki.org/cgi-bin/view/Codev/DownloadTWiki">http://twiki.org/cgi-bin/view/Codev/DownloadTWiki</a>	
<b>Affected Software/OS</b> TWiki version prior to 4.3.1	
<b>Vulnerability Insight</b> 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.	
<b>Vulnerability Detection Method</b> Details:TWiki Cross-Site Request Forgery Vulnerability OID:1.3.6.1.4.1.25623.1.0.800400 Version used: \$Revision: 4892 \$	
<b>Product Detection Result</b> Product: cpe:/a:twiki:twiki:01.Feb.2003 Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)	
<b>References</b> CVE: CVE-2009-1339 Other: URL: <a href="http://secunia.com/advisories/34880">http://secunia.com/advisories/34880</a> URL: <a href="http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258">http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258</a> URL: <a href="http://twiki.org/pub/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di">http://twiki.org/pub/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di</a> ↪ff-cve-2009-1339.txt	
Medium (CVSS: 5.8) NVT: http TRACE XSS attack	
<b>Summary</b> 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.	
<b>Vulnerability Detection Result</b> <b>Solution:</b>	
... continues on next page ...	

<p>...continued from previous page...</p> <p>Add the following lines for each virtual host in your configuration file :</p> <pre>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE TRACK) RewriteRule .* - [F]</pre> <p>See also <a href="http://httpd.apache.org/docs/current/de/mod/core.html#traceenable">http://httpd.apache.org/docs/current/de/mod/core.html#traceenable</a></p>
<p><b>Solution</b></p> <p>Disable these methods.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Details:http TRACE XSS attack  OID:1.3.6.1.4.1.25623.1.0.11213  Version used: \$Revision: 6063 \$</p>
<p><b>References</b></p> <p>CVE: CVE-2004-2320, CVE-2003-1567    BID:9506, 9561, 11604    Other:    URL:<a href="http://www.kb.cert.org/vuls/id/867593">http://www.kb.cert.org/vuls/id/867593</a></p>

<p>Medium (CVSS: 5.0)  NVT: /doc directory browsable</p>
<p><b>Summary</b></p> <p>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.</p>
<p><b>Vulnerability Detection Result</b></p> <p>Vulnerable url: <a href="http://192.168.56.101/doc/">http://192.168.56.101/doc/</a></p>
<p><b>Solution</b></p> <p><b>Solution type:</b> Mitigation</p> <p>Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:</p> <pre>&lt;Directory /usr/doc&gt; AllowOverride None order deny,allow deny from all allow from localhost &lt;/Directory&gt;</pre>
<p><b>Vulnerability Detection Method</b></p> <p>Details:/doc directory browsable  OID:1.3.6.1.4.1.25623.1.0.10056  Version used: \$Revision: 4288 \$</p>
<p><b>References</b></p> <p>CVE: CVE-1999-0678    BID:318</p>



<p>Medium (CVSS: 4.3)  NVT: phpMyAdmin SQL bookmark XSS Vulnerability</p>
<p><b>Product detection result</b>  cpe:/a:phpmyadmin:phpmyadmin:3.1.1  Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p><b>Summary</b>  This host is running phpMyAdmin and is prone to Cross Site Scripting vulnerability.</p>
<p><b>Vulnerability Detection Result</b>  Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p><b>Impact</b>  Successful exploitation will let the attacker cause XSS attacks and inject malicious web script or HTML code via a crafted SQL bookmarks.</p>
<p><b>Solution</b>  Apply the respective patches or upgrade to version 3.2.0.1  <a href="http://www.phpmyadmin.net/home_page/downloads.php">http://www.phpmyadmin.net/home_page/downloads.php</a> <a href="http://phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin/trunk/patches/3.2.0.1/">http://phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin/trunk/patches/3.2.0.1/</a>  *** Note: Ignore the warning if above mentioned patches are applied. *****</p>
<p><b>Affected Software/OS</b>  phpMyAdmin version 3.0.x to 3.2.0.rc1</p>
<p><b>Vulnerability Insight</b>  This flaw arises because the input passed into SQL bookmarks is not adequately sanitised before using it in dynamically generated content.</p>
<p><b>Vulnerability Detection Method</b>  Details:phpMyAdmin SQL bookmark XSS Vulnerability  OID:1.3.6.1.4.1.25623.1.0.800595  Version used: \$Revision: 4869 \$</p>
<p><b>Product Detection Result</b>  Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1  Method: phpMyAdmin Detection  OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p><b>References</b>  CVE: CVE-2009-2284  BID:35543  Other:  URL:<a href="http://secunia.com/advisories/35649">http://secunia.com/advisories/35649</a>  URL:<a href="http://www.phpmyadmin.net/home_page/security/PMASA-2009-5.php">http://www.phpmyadmin.net/home_page/security/PMASA-2009-5.php</a></p>

Medium (CVSS: 4.3) NVT: phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities
<b>Product detection result</b> cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Solution</b> Vendor updates are available. Please see the references for details.
<b>Vulnerability Detection Method</b> 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 \$
<b>Product Detection Result</b> Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
<b>References</b> 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 Multiple Cross Site Scripting Vulnerabilities
<b>Product detection result</b> cpe:/a:phpmyadmin:phpmyadmin:3.1.1 ... continues on next page ...

...continued from previous page ...
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
<b>Summary</b> <p>phpMyAdmin is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.</p> <p>An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks.</p> <p>The following versions are vulnerable:</p> <p>phpMyAdmin 2.11.x prior to 2.11.10.1 phpMyAdmin 3.x prior to 3.3.5.1</p>
<b>Vulnerability Detection Result</b> <p>Vulnerability was detected according to the Vulnerability Detection Method.</p>
<b>Solution</b> <p>Updates are available. Please see the references for details.</p>
<b>Vulnerability Detection Method</b> <p>Details:phpMyAdmin Multiple Cross Site Scripting Vulnerabilities</p> <p>OID:1.3.6.1.4.1.25623.1.0.100761</p> <p>Version used: \$Revision: 5323 \$</p>
<b>Product Detection Result</b> <p>Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1</p> <p>Method: phpMyAdmin Detection</p> <p>OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<b>References</b> <p>CVE: CVE-2010-3056</p> <p>BID:42584</p> <p>Other:</p> <p>URL:https://www.securityfocus.com/bid/42584</p> <p>URL:http://www.phpmyadmin.net/</p> <p>URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-5.php</p>

Medium (CVSS: 4.3)
NVT: phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability
<b>Product detection result</b> <p>cpe:/a:phpmyadmin:phpmyadmin:3.1.1</p> <p>Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<b>Summary</b> <p>... continues on next page ...</p>

...continued from previous page ...
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> 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
<b>Solution</b> Upgrade to phpMyAdmin version 3.3.7 or later, For updates refer to <a href="http://www.phpmyadmin.net/home_page/downloads.php">http://www.phpmyadmin.net/home_page/downloads.php</a>
<b>Affected Software/OS</b> phpMyAdmin versions 3.x before 3.3.7
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Details:phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability OID:1.3.6.1.4.1.25623.1.0.801286 Version used: \$Revision: 5373 \$
<b>Product Detection Result</b> Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
<b>References</b> CVE: CVE-2010-3263 Other: URL: <a href="http://secunia.com/advisories/41210">http://secunia.com/advisories/41210</a> URL: <a href="http://xforce.iss.net/xforce/xfdb/61675">http://xforce.iss.net/xforce/xfdb/61675</a> URL: <a href="http://www.phpmyadmin.net/home_page/security/PMASA-2010-7.php">http://www.phpmyadmin.net/home_page/security/PMASA-2010-7.php</a>
Medium (CVSS: 4.3) NVT: phpMyAdmin Database Search Cross Site Scripting Vulnerability
<b>Product detection result</b> cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
... continues on next page ...

...continued from previous page ...
<p><b>Summary</b>  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.</p>
<p><b>Vulnerability Detection Result</b>  Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p><b>Solution</b>  Vendor updates are available. Please see the references for more information.</p>
<p><b>Vulnerability Detection Method</b>  Details:phpMyAdmin Database Search Cross Site Scripting Vulnerability  OID:1.3.6.1.4.1.25623.1.0.100939  Version used: \$Revision: 5323 \$</p>
<p><b>Product Detection Result</b>  Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1  Method: phpMyAdmin Detection  OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p><b>References</b>  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</p>
<p>Medium (CVSS: 4.3)  NVT: phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability</p>
<p><b>Product detection result</b>  cpe:/a:phpmyadmin:phpmyadmin:3.1.1  Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p><b>Summary</b>  phpMyAdmin is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.</p>
... continues on next page ...

...continued from previous page ...
<p>An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.</p> <p>Versions prior to phpMyAdmin 3.3.6 are vulnerable other versions may also be affected.</p>
<p><b>Vulnerability Detection Result</b></p> <p>Vulnerability was detected according to the Vulnerability Detection Method.</p>
<p><b>Solution</b></p> <p>Vendor updates are available. Please see the references for more information.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Details:phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability  OID:1.3.6.1.4.1.25623.1.0.100775  Version used: \$Revision: 5323 \$</p>
<p><b>Product Detection Result</b></p> <p>Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1  Method: phpMyAdmin Detection  OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p><b>References</b></p> <p>CVE: CVE-2010-2958  BID:42874  Other:  URL:https://www.securityfocus.com/bid/42874  URL:http://www.phpmyadmin.net/  URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-6.php  URL:http://www.phpmyadmin.git.sourceforge.net/git/gitweb.cgi?p=phpmyadmin/php  ↪myadmin;a=commitdiff;h=133a77fac7d31a38703db2099a90c1b49de62e37</p>
<p>Medium (CVSS: 4.3)  NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability</p>
<p><b>Product detection result</b></p> <p>cpe:/a:phpmyadmin:phpmyadmin:3.1.1  Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)</p>
<p><b>Summary</b></p> <p>The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.</p>
<p><b>Vulnerability Detection Result</b></p> <p>Vulnerability was detected according to the Vulnerability Detection Method.</p>
... continues on next page ...

...continued from previous page ...
<b>Impact</b> Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks. Impact Level: Application
<b>Solution</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> phpMyAdmin version 3.3.8.1 and prior.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Details:phpMyAdmin 'error.php' Cross Site Scripting Vulnerability OID:1.3.6.1.4.1.25623.1.0.801660 Version used: \$Revision: 5323 \$
<b>Product Detection Result</b> Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 Method: phpMyAdmin Detection OID: 1.3.6.1.4.1.25623.1.0.900129)
<b>References</b> CVE: CVE-2010-4480 Other: URL: <a href="http://www.exploit-db.com/exploits/15699/">http://www.exploit-db.com/exploits/15699/</a> URL: <a href="http://www.vupen.com/english/advisories/2010/3133">http://www.vupen.com/english/advisories/2010/3133</a>
Medium (CVSS: 4.3) NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
<b>Summary</b> This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
... continues on next page ...

...continued from previous page ...
<b>Impact</b> Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks. Impact Level: Application
<b>Solution</b> <b>Solution type:</b> VendorFix Upgrade to Apache HTTP Server version 2.2.22 or later, For updates refer to <a href="http://httpd.apache.org/">http://httpd.apache.org/</a>
<b>Affected Software/OS</b> Apache HTTP Server versions 2.2.0 through 2.2.21
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Details:Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.902830 Version used: \$Revision: 5950 \$
<b>References</b> CVE: CVE-2012-0053 BID:51706 Other: URL: <a href="http://secunia.com/advisories/47779">http://secunia.com/advisories/47779</a> URL: <a href="http://www.exploit-db.com/exploits/18442">http://www.exploit-db.com/exploits/18442</a> URL: <a href="http://rhn.redhat.com/errata/RHSA-2012-0128.html">http://rhn.redhat.com/errata/RHSA-2012-0128.html</a> URL: <a href="http://httpd.apache.org/security/vulnerabilities_22.html">http://httpd.apache.org/security/vulnerabilities_22.html</a> URL: <a href="http://svn.apache.org/viewvc?view=revision&amp;revision=1235454">http://svn.apache.org/viewvc?view=revision&amp;revision=1235454</a> URL: <a href="http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm">http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm</a> ↩1

[ [return to 192.168.56.101](#) ]

### 2.1.15 Medium 25/tcp

Medium (CVSS: 6.8) NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability
<b>Summary</b> Multiple vendors' implementations of STARTTLS are prone to a vulnerability that lets attackers inject arbitrary commands.
... continues on next page ...



...continued from previous page ...
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> An attacker can exploit this issue to execute arbitrary commands in the context of the user running the application. Successful exploits can allow attackers to obtain email usernames and passwords.
<b>Solution</b> Updates are available.
<b>Affected Software/OS</b> The following vendors are affected: Ipswitch Kerio Postfix Qmail-TLS Oracle SCO Group spamdyke ISC
<b>Vulnerability Detection Method</b> Send a special crafted STARTTLS request and check the response. Details: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection . ↔.. OID: 1.3.6.1.4.1.25623.1.0.103935 Version used: \$Revision: 2780 \$
<b>References</b> CVE: CVE-2011-0411, CVE-2011-1430, CVE-2011-1431, CVE-2011-1432, CVE-2011-1575, ↔ CVE-2011-1926, CVE-2011-2165 BID: 46767 Other: URL: <a href="http://www.securityfocus.com/bid/46767">http://www.securityfocus.com/bid/46767</a> URL: <a href="http://kolab.org/pipermail/kolab-announce/2011/000101.html">http://kolab.org/pipermail/kolab-announce/2011/000101.html</a> URL: <a href="http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424">http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424</a> URL: <a href="http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7">http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7</a> URL: <a href="http://www.kb.cert.org/vuls/id/MAPG-8D9M4P">http://www.kb.cert.org/vuls/id/MAPG-8D9M4P</a> URL: <a href="http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-↔notes.txt">http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-↔notes.txt</a> URL: <a href="http://www.postfix.org/CVE-2011-0411.html">http://www.postfix.org/CVE-2011-0411.html</a> URL: <a href="http://www.pureftpd.org/project/pure-ftpd/news">http://www.pureftpd.org/project/pure-ftpd/news</a> URL: <a href="http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNot↔es_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf">http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNot↔es_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf</a> URL: <a href="http://www.spamdyke.org/documentation/Changelog.txt">http://www.spamdyke.org/documentation/Changelog.txt</a> URL: <a href="http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?inclu↔de_text=1">http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?inclu↔de_text=1</a> URL: <a href="http://www.securityfocus.com/archive/1/516901">http://www.securityfocus.com/archive/1/516901</a> URL: <a href="http://support.avaya.com/css/P8/documents/100134676">http://support.avaya.com/css/P8/documents/100134676</a> URL: <a href="http://support.avaya.com/css/P8/documents/100141041">http://support.avaya.com/css/P8/documents/100141041</a> URL: <a href="http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html">http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html</a> URL: <a href="http://inoa.net/qmail-tls/vu555316.patch">http://inoa.net/qmail-tls/vu555316.patch</a>
... continues on next page ...

...continued from previous page ...

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

Medium (CVSS: 5.0)

NVT: Check if Mailserver answer to VRFY and EXPN requests

**Summary**

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

**Vulnerability Detection Result**

'VRFY root' produces the following answer: 252 2.0.0 root

**Solution**

**Solution type:** Workaround

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'.

**Vulnerability Detection Method**

Details: Check if Mailserver answer to VRFY and EXPN requests

OID: 1.3.6.1.4.1.25623.1.0.100072

Version used: \$Revision: 5899 \$

**References**

Other:

URL: <http://cr.yp.to/smtp/vrfy.html>

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

**Summary**

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

**Vulnerability Detection Result**

The certificate of the remote service expired on 2010-04-16 14:07:45.

Certificate details:

```
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
```

subject alternative names (SAN):

None

issued by ..: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6

... continues on next page ...

...continued from previous page ...
<pre> ↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of ↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid ↪e US,C=XX serial .....: 00FAF93A4C7FB6B9CC valid from : 2010-03-17 14:07:45 UTC valid until: 2010-04-16 14:07:45 UTC fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6 fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436 ↪DE813CC </pre>
<b>Solution</b> <b>Solution type:</b> Mitigation Replace the SSL/TLS certificate by a new one.
<b>Vulnerability Insight</b> This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.
<b>Vulnerability Detection Method</b> Details:SSL/TLS: Certificate Expired OID:1.3.6.1.4.1.25623.1.0.103955 Version used: \$Revision: 4765 \$

Medium (CVSS: 4.3) NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
<b>Summary</b> It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
<b>Vulnerability Detection Result</b> In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and S ↪SLv3 protocols and supports one or more ciphers. Those supported ciphers can b ↪e found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1. ↪25623.1.0.802067) NVT.
<b>Impact</b> 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.
<b>Solution</b> <b>Solution type:</b> 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.
... continues on next page ...

...continued from previous page...	
<b>Affected Software/OS</b>	All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
<b>Vulnerability Insight</b>	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)
<b>Vulnerability Detection Method</b>	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 \$
<b>References</b>	CVE: CVE-2016-0800, CVE-2014-3566 Other: URL: <a href="https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report">https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report</a> URL: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> URL: <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a> URL: <a href="https://drownattack.com/">https://drownattack.com/</a> URL: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a>
Medium (CVSS: 4.3) NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)	
<b>Summary</b>	This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.
<b>Vulnerability Detection Result</b>	'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
<b>Impact</b>	Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application
<b>Solution</b>	...
... continues on next page ...	

...continued from previous page ...
<b>Solution type:</b> VendorFix - Remove support for 'DHE_EXPORT' cipher suites from the service - If running OpenSSL update to version 1.0.2b or 1.0.1n or later, For updates refer to <a href="https://www.openssl.org">https://www.openssl.org</a>
<b>Affected Software/OS</b> - Hosts accepting 'DHE_EXPORT' cipher suites - OpenSSL version before 1.0.2b and 1.0.1n
<b>Vulnerability Insight</b> Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.
<b>Vulnerability Detection Method</b> Check previous collected cipher suites saved in the KB. Details:SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) OID:1.3.6.1.4.1.25623.1.0.805188 Version used: \$Revision: 4781 \$
<b>References</b> CVE: CVE-2015-4000 BID:74733 Other: URL: <a href="https://weakdh.org">https://weakdh.org</a> URL: <a href="https://weakdh.org/imperfect-forward-secrecy.pdf">https://weakdh.org/imperfect-forward-secrecy.pdf</a> URL: <a href="http://openwall.com/lists/oss-security/2015/05/20/8">http://openwall.com/lists/oss-security/2015/05/20/8</a> URL: <a href="https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained">https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained</a> URL: <a href="https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-change">https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-change</a> ↪s
Medium (CVSS: 4.3) NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
<b>Summary</b> This host is prone to an information disclosure vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application
<b>Solution</b> ... continues on next page ...

...continued from previous page ...	
<b>Solution type:</b> Mitigation Possible Mitigations are: <ul style="list-style-type: none"> <li>- Disable SSLv3</li> <li>- Disable cipher suites supporting CBC cipher modes</li> <li>- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+</li> </ul>	
<b>Vulnerability Insight</b> The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code	
<b>Vulnerability Detection Method</b> 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 \$	
<b>References</b> CVE: CVE-2014-3566 BID:70574 Other: <ul style="list-style-type: none"> <li>URL:<a href="https://www.openssl.org/~bodo/ssl-poodle.pdf">https://www.openssl.org/~bodo/ssl-poodle.pdf</a></li> <li>URL:<a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a></li> <li>URL:<a href="https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html">https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html</a></li> <li>URL:<a href="http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit-ing-ssl-30.html">http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit-ing-ssl-30.html</a></li> </ul>	
Medium (CVSS: 4.3) NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	
<b>Summary</b> This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.	
<b>Vulnerability Detection Result</b> 'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol: <ul style="list-style-type: none"> <li>TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA</li> <li>TLS_RSA_EXPORT_WITH_DES40_CBC_SHA</li> <li>TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5</li> <li>TLS_RSA_EXPORT_WITH_RC4_40_MD5</li> </ul> 'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol: <ul style="list-style-type: none"> <li>TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA</li> <li>TLS_RSA_EXPORT_WITH_DES40_CBC_SHA</li> <li>TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5</li> <li>TLS_RSA_EXPORT_WITH_RC4_40_MD5</li> </ul>	
<b>Impact</b> ... continues on next page ...	

...continued from previous page ...
<p>Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.</p> <p>Impact Level: Application</p>
<p><b>Solution</b></p> <p><b>Solution type:</b> VendorFix</p> <ul style="list-style-type: none"> <li>- Remove support for 'RSA_EXPORT' cipher suites from the service.</li> <li>- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later For updates refer to <a href="https://www.openssl.org">https://www.openssl.org</a></li> </ul>
<p><b>Affected Software/OS</b></p> <ul style="list-style-type: none"> <li>- Hosts accepting 'RSA_EXPORT' cipher suites</li> <li>- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.</li> </ul>
<p><b>Vulnerability Insight</b></p> <p>Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Check previous collected cipher suites saved in the KB.</p> <p>Details:SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)</p> <p>OID:1.3.6.1.4.1.25623.1.0.805142</p> <p>Version used: \$Revision: 4781 \$</p>
<p><b>References</b></p> <p>CVE: CVE-2015-0204</p> <p>BID:71936</p> <p>Other:</p> <ul style="list-style-type: none"> <li>URL:<a href="https://freakattack.com">https://freakattack.com</a></li> <li>URL:<a href="http://secpod.org/blog/?p=3818">http://secpod.org/blog/?p=3818</a></li> <li>URL:<a href="http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-f-actoring-nsa.html">http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-f-actoring-nsa.html</a></li> </ul>
<p>Medium (CVSS: 4.0)</p> <p>NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm</p>
<p><b>Summary</b></p> <p>The remote service is using a SSL/TLS certificate chain that has been signed using a cryptographically weak hashing algorithm.</p>
<p><b>Vulnerability Detection Result</b></p> <p>The following certificates are part of the certificate chain but using insecure ↪signature algorithms:</p> <p>Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173</p> <p>↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic</p> <p>... continues on next page ...</p>

...continued from previous page ...
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi ↪ng outside US,C=XX Signature Algorithm: sha1WithRSAEncryption
<b>Solution</b> <b>Solution type:</b> 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.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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 \$
<b>References</b> <b>Other:</b> URL: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</a>

Medium (CVSS: 4.0) NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
<b>Summary</b> The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
<b>Vulnerability Detection Result</b> Server Temporary Key Size: 1024 bits
<b>Impact</b> An attacker might be able to decrypt the SSL/TLS communication offline.
<b>Solution</b> <b>Solution type:</b> Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a> ). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
<b>Vulnerability Insight</b> ... continues on next page ...



...continued from previous page ...
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.
<b>Vulnerability Detection Method</b> 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: 6114 \$
<b>References</b> Other: URL:https://weakdh.org/ URL:https://weakdh.org/sysadmin.html

[ [return to 192.168.56.101](#) ]

### 2.1.16 Medium 445/tcp

Medium (CVSS: 6.0) NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)
<b>Product detection result</b> cpe:/a:samba:samba:3.0.20 Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)
<b>Summary</b> Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.
<b>Solution</b> <b>Solution type:</b> VendorFix Updates are available. Please see the referenced vendor advisory.
<b>Affected Software/OS</b> This issue affects Samba 3.0.0 to 3.0.25rc3.
... continues on next page ...

...continued from previous page ...

**Vulnerability Detection Method**

Send a crafted command to the samba server and check for a remote command execution.

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

OID:1.3.6.1.4.1.25623.1.0.108011

Version used: \$Revision: 4401 \$

**Product Detection Result**

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

Method: SMB NativeLanMan

OID: 1.3.6.1.4.1.25623.1.0.102011)

**References**

CVE: CVE-2007-2447

BID:23972

Other:

URL:http://www.securityfocus.com/bid/23972

URL:https://www.samba.org/samba/security/CVE-2007-2447.html

[\[ return to 192.168.56.101 \]](#)**2.1.17 Medium 22/tcp**

Medium (CVSS: 4.3)

NVT: SSH Weak Encryption Algorithms Supported

**Summary**

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

**Vulnerability Detection Result**The following weak client-to-server encryption algorithms are supported by the r  
↪emote service:

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

The following weak server-to-client encryption algorithms are supported by the r  
↪emote service:

3des-cbc

... continues on next page ...

...continued from previous page ...
aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se
<b>Solution</b> <b>Solution type:</b> Mitigation Disable the weak encryption algorithms.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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 \$
<b>References</b> Other: URL: <a href="https://tools.ietf.org/html/rfc4253#section-6.3">https://tools.ietf.org/html/rfc4253#section-6.3</a> URL: <a href="https://www.kb.cert.org/vuls/id/958563">https://www.kb.cert.org/vuls/id/958563</a>

[ [return to 192.168.56.101](#) ]

### 2.1.18 Medium 5432/tcp

Medium (CVSS: 6.8) NVT: PostgreSQL Multiple Security Vulnerabilities
<b>Product detection result</b> 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 ...
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Solution</b> Updates are available. Please see the references for more information.
<b>Vulnerability Detection Method</b> Details:PostgreSQL Multiple Security Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.100273 Version used: \$Revision: 5016 \$
<b>Product Detection Result</b> Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>References</b> CVE: CVE-2009-3229, CVE-2009-3230, CVE-2009-3231 BID:36314 Other: URL:http://www.securityfocus.com/bid/36314 URL:https://bugzilla.redhat.com/show_bug.cgi?id=522085#c1 URL:http://www.postgresql.org/ URL:http://www.postgresql.org/support/security URL:http://permalink.gmane.org/gmane.comp.security.oss.general/2088
Medium (CVSS: 6.8) NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
<b>Summary</b> OpenSSL is prone to security-bypass vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> ... continues on next page ...

...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.
<b>Solution</b> <b>Solution type:</b> VendorFix Updates are available.
<b>Affected Software/OS</b> OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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 \$
<b>References</b> CVE: CVE-2014-0224 BID:67899 Other: URL:http://www.securityfocus.com/bid/67899 URL:http://openssl.org/

Medium (CVSS: 6.5)

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

#### Product detection result

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.

... continues on next page ...

...continued from previous page ...
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.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Solution</b> Updates are available. Please see the references for more information.
<b>Vulnerability Detection Method</b> 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 \$
<b>Product Detection Result</b> Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>References</b> CVE: CVE-2009-4034, CVE-2009-4136 BID:37334, 37333 Other: URL:http://www.securityfocus.com/bid/37334 URL:http://www.securityfocus.com/bid/37333 URL:http://www.postgresql.org URL:http://www.postgresql.org/support/security URL:http://www.postgresql.org/about/news.1170
Medium (CVSS: 6.5) NVT: PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability
<b>Product detection result</b> cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> ... continues on next page ...

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

Medium (CVSS: 6.5) NVT: PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability
<b>Product detection result</b> cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Vulnerability Detection Method</b> Details:PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.100470 Version used: \$Revision: 5394 \$
... continues on next page ...

...continued from previous page ...
<b>Product Detection Result</b> Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>References</b> 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: 6.0) NVT: PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability
<b>Product detection result</b> cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Solution</b> Updates are available. Please see the references for more information.
<b>Vulnerability Detection Method</b> 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 \$
<b>Product Detection Result</b> Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
... continues on next page ...



...continued from previous page ...

**References**

CVE: CVE-2010-3433

BID: 43747

Other:

URL: <https://www.securityfocus.com/bid/43747>URL: <http://www.postgresql.org/docs/9.0/static/release-9-0-1.html>URL: <http://www.postgresql.org>URL: <http://www.postgresql.org/support/security>

Medium (CVSS: 5.5)

NVT: PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability

**Product detection result**

cpe:/a:postgresql:postgresql:8.3.1

Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

**Summary**

PostgreSQL is prone to an unauthorized-access vulnerability.

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

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Solution**

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

**Vulnerability Detection Method**

Details: PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.100648

Version used: \$Revision: 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-2010-1975

BID: 40304

Other:

URL: <http://www.securityfocus.com/bid/40304>

... continues on next page ...

...continued from previous page...

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

Medium (CVSS: 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: Deprecated SSLv2 and SSLv3 Protocol Detection
<b>Summary</b> It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
<b>Vulnerability Detection Result</b> 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.
<b>Impact</b> 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.
<b>Solution</b> <b>Solution type:</b> 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.
<b>Affected Software/OS</b> All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
<b>Vulnerability Insight</b> 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)
<b>Vulnerability Detection Method</b> 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 \$
<b>References</b> CVE: CVE-2016-0800, CVE-2014-3566 Other: URL: <a href="https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report">https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report</a> URL: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> URL: <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a> URL: <a href="https://drownattack.com/">https://drownattack.com/</a> URL: <a href="https://www.imperialviolet.org/2014/10/14/poodle.html">https://www.imperialviolet.org/2014/10/14/poodle.html</a>

Medium (CVSS: 4.3) NVT: SSL/TLS: Report Weak Cipher Suites
<b>Summary</b> This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
<b>Vulnerability Detection Result</b> 'Weak' cipher suites accepted by this service via the SSLv3 protocol: TLS_RSA_WITH_RC4_128_SHA 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_SHA
<b>Solution</b> <b>Solution type:</b> Mitigation The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.
<b>Vulnerability Insight</b> These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000). - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong
<b>Vulnerability Detection Method</b> Details:SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: \$Revision: 5525 \$
<b>References</b> CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000 Other: URL: <a href="https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html">https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html</a> URL: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> URL: <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a>

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

...continued from previous page ...	
<b>Summary</b>	This host is prone to an information disclosure vulnerability.
<b>Vulnerability Detection Result</b>	Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b>	Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application
<b>Solution</b>	<b>Solution type:</b> Mitigation Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
<b>Vulnerability Insight</b>	The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
<b>Vulnerability Detection Method</b>	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 \$
<b>References</b>	CVE: CVE-2014-3566 BID:70574 Other: URL:https://www.openssl.org/~bodo/ssl-poodle.pdf URL:https://www.imperialviolet.org/2014/10/14/poodle.html URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit- ↔ing-ssl-30.html
Medium (CVSS: 4.0) NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	
<b>Summary</b>	The remote service is using a SSL/TLS certificate chain that has been signed using a cryptographically weak hashing algorithm.
... continues on next page ...	

...continued from previous page ...
<b>Vulnerability Detection Result</b> 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
<b>Solution</b> <b>Solution type:</b> 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.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> 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 \$
<b>References</b> <b>Other:</b> URL: <a href="https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</a>

Medium (CVSS: 4.0) NVT: PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability
<b>Product detection result</b> cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
... continues on next page ...

...continued from previous page...
<b>Solution</b> Updates are available. Update to newer Version.
<b>Vulnerability Detection Method</b> Details:PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability OID:1.3.6.1.4.1.25623.1.0.100157 Version used: \$Revision: 5016 \$
<b>Product Detection Result</b> Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>References</b> CVE: CVE-2009-0922 BID:34090 Other: URL: <a href="http://www.securityfocus.com/bid/34090">http://www.securityfocus.com/bid/34090</a> URL: <a href="http://www.postgresql.org/">http://www.postgresql.org/</a>

Medium (CVSS: 4.0) NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
<b>Summary</b> The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
<b>Vulnerability Detection Result</b> Server Temporary Key Size: 1024 bits
<b>Impact</b> An attacker might be able to decrypt the SSL/TLS communication offline.
<b>Solution</b> <b>Solution type:</b> Workaround Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a> ). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
<b>Vulnerability Insight</b> The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.
... continues on next page ...

...continued from previous page ...
<b>Vulnerability Detection Method</b> 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: 6114 \$
<b>References</b> Other: URL:https://weakdh.org/ URL:https://weakdh.org/sysadmin.html

[ [return to 192.168.56.101](#) ]

### 2.1.19 Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 152069 Packet 2: 152181
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.
<b>Solution</b> <b>Solution type:</b> 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: <a href="http://www.microsoft.com/en-us/download/details.aspx?id=9152">http://www.microsoft.com/en-us/download/details.aspx?id=9152</a>
<b>Affected Software/OS</b> TCP/IPv4 implementations that implement RFC1323.
... continues on next page ...



...continued from previous page...

**Vulnerability Insight**

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

**Vulnerability Detection Method**

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

Details:TCP timestamps

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: \$Revision: 5740 \$

**References**

Other:

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

[\[ return to 192.168.56.101 \]](#)

**2.1.20 Low 22/tcp**

Low (CVSS: 2.6)

NVT: SSH Weak MAC Algorithms Supported

**Summary**

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

**Vulnerability Detection Result**

The following weak client-to-server MAC algorithms are supported by the remote s  
↪ervice:

hmac-md5

hmac-md5-96

hmac-sha1-96

The following weak server-to-client MAC algorithms are supported by the remote s  
↪ervice:

hmac-md5

hmac-md5-96

hmac-sha1-96

**Solution**

**Solution type:** Mitigation

Disable the weak MAC algorithms.

**Vulnerability Detection Method**

Details:SSH Weak MAC Algorithms Supported

OID:1.3.6.1.4.1.25623.1.0.105610

Version used: \$Revision: 4490 \$

[\[ return to 192.168.56.101 \]](#)

### 2.1.21 Low 5432/tcp

Low (CVSS: 3.5) NVT: PostgreSQL Hash Table Integer Overflow Vulnerability
<b>Product detection result</b> cpe:/a:postgresql:postgresql:8.3.1 Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>Summary</b> The host is running PostgreSQL and is prone to integer overflow vulnerability.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> 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
<b>Solution</b> Apply the patch, <a href="http://git.postgresql.org/gitweb?p=postgresql.git">http://git.postgresql.org/gitweb?p=postgresql.git</a> a=commitdiff h=64b057e6823655fb6c5d1f24a28f236b94dd6c54 **** NOTE: Please ignore this warning if the patch is applied. ****
<b>Affected Software/OS</b> PostgreSQL version 8.4.1 and prior and 8.5 through 8.5alpha2
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Details:PostgreSQL Hash Table Integer Overflow Vulnerability OID:1.3.6.1.4.1.25623.1.0.902139 Version used: \$Revision: 5401 \$
<b>Product Detection Result</b> Product: cpe:/a:postgresql:postgresql:8.3.1 Method: PostgreSQL Detection OID: 1.3.6.1.4.1.25623.1.0.100151)
<b>References</b> CVE: CVE-2010-0733 ... continues on next page ...

...continued from previous page ...

**Other:**

URL:[https://bugzilla.redhat.com/show\\_bug.cgi?id=546621](https://bugzilla.redhat.com/show_bug.cgi?id=546621)  
 URL:<http://www.openwall.com/lists/oss-security/2010/03/16/10>  
 URL:<http://archives.postgresql.org/pgsql-bugs/2009-10/msg00310.php>  
 URL:<http://archives.postgresql.org/pgsql-bugs/2009-10/msg00289.php>  
 URL:<http://archives.postgresql.org/pgsql-bugs/2009-10/msg00287.php>  
 URL:<http://archives.postgresql.org/pgsql-bugs/2009-10/msg00277.php>

Low (CVSS: 2.1)

NVT: PostgreSQL Low Cost Function Information Disclosure Vulnerability

**Product detection result**

cpe:/a:postgresql:postgresql:8.3.1

Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

**Summary**

PostgreSQL is prone to an information-disclosure vulnerability.

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.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Vulnerability Detection Method**

Details:PostgreSQL Low Cost Function Information Disclosure Vulnerability

OID:1.3.6.1.4.1.25623.1.0.100158

Version used: \$Revision: 5016 \$

**Product Detection Result**

Product: cpe:/a:postgresql:postgresql:8.3.1

Method: PostgreSQL Detection

OID: 1.3.6.1.4.1.25623.1.0.100151)

**References**

BID:34069

**Other:**URL:<http://www.securityfocus.com/bid/34069>URL:<http://www.postgresql.org/>[\[ return to 192.168.56.101 \]](#)

This file was automatically generated.