

# Scan Report

November 30, 2019

## 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 “full scan”. The scan started at Sat Nov 30 11:38:05 2019 UTC and ended at Sat Nov 30 12:10:43 2019 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	10.0.2.4 . . . . .	2
2.1.1	High 22/tcp . . . . .	3
2.1.2	High 3306/tcp . . . . .	4
2.1.3	High 5900/tcp . . . . .	4
2.1.4	High 1524/tcp . . . . .	5
2.1.5	High 513/tcp . . . . .	5
2.1.6	High 6667/tcp . . . . .	6
2.1.7	High 8787/tcp . . . . .	7
2.1.8	High general/tcp . . . . .	8
2.1.9	High 21/tcp . . . . .	9
2.1.10	High 3632/tcp . . . . .	10
2.1.11	High 80/tcp . . . . .	11
2.1.12	High 512/tcp . . . . .	14
2.1.13	High 5432/tcp . . . . .	15
2.1.14	High 6200/tcp . . . . .	16
2.1.15	Medium 22/tcp . . . . .	17
2.1.16	Medium 5900/tcp . . . . .	18
2.1.17	Medium 445/tcp . . . . .	19

2.1.18	Medium 6667/tcp . . . . .	20
2.1.19	Medium 2121/tcp . . . . .	21
2.1.20	Medium 25/tcp . . . . .	22
2.1.21	Medium 21/tcp . . . . .	31
2.1.22	Medium 80/tcp . . . . .	32
2.1.23	Medium 23/tcp . . . . .	42
2.1.24	Medium 5432/tcp . . . . .	42
2.1.25	Low 22/tcp . . . . .	49
2.1.26	Low general/tcp . . . . .	49

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
<a href="#">10.0.2.4</a>	17	34	2	0	0
Total: 1	17	34	2	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 53 results selected by the filtering described above. Before filtering there were 396 results.

### 1.1 Host Authentications

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

## 2 Results per Host

### 2.1 10.0.2.4

Host scan start Sat Nov 30 11:38:14 2019 UTC

Host scan end Sat Nov 30 12:10:43 2019 UTC

Service (Port)	Threat Level
<a href="#">22/tcp</a>	High
<a href="#">3306/tcp</a>	High
<a href="#">5900/tcp</a>	High
<a href="#">1524/tcp</a>	High
<a href="#">513/tcp</a>	High
<a href="#">6667/tcp</a>	High
<a href="#">8787/tcp</a>	High
<a href="#">general/tcp</a>	High
<a href="#">21/tcp</a>	High
<a href="#">3632/tcp</a>	High

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
<a href="#">80/tcp</a>	High
<a href="#">512/tcp</a>	High
<a href="#">5432/tcp</a>	High
<a href="#">6200/tcp</a>	High
<a href="#">22/tcp</a>	Medium
<a href="#">5900/tcp</a>	Medium
<a href="#">445/tcp</a>	Medium
<a href="#">6667/tcp</a>	Medium
<a href="#">2121/tcp</a>	Medium
<a href="#">25/tcp</a>	Medium
<a href="#">21/tcp</a>	Medium
<a href="#">80/tcp</a>	Medium
<a href="#">23/tcp</a>	Medium
<a href="#">5432/tcp</a>	Medium
<a href="#">22/tcp</a>	Low
<a href="#">general/tcp</a>	Low

### 2.1.1 High 22/tcp

High (CVSS: 7.5)

NVT: SSH Brute Force Logins With Default Credentials Reporting

#### Summary

It was possible to login into the remote SSH server using default credentials.

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

#### Vulnerability Detection Result

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

#### Solution

**Solution type:** Mitigation

Change the password as soon as possible.

#### Vulnerability Detection Method

Try to login with a number of known default credentials via the SSH protocol.

Details: SSH Brute Force Logins With Default Credentials Reporting

OID:1.3.6.1.4.1.25623.1.0.103239

Version used: 2019-09-06T14:17:49+0000

[\[ return to 10.0.2.4 \]](#)

**2.1.2 High 3306/tcp**

High (CVSS: 9.0) NVT: MySQL / MariaDB weak password
<b>Product detection result</b> cpe:/a:mysql:mysql:5.0.51a Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
<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: 2019-09-06T14:17:49+0000
<b>Product Detection Result</b> Product: cpe:/a:mysql:mysql:5.0.51a Method: MySQL/MariaDB Detection OID: 1.3.6.1.4.1.25623.1.0.100152)

[\[ return to 10.0.2.4 \]](#)

**2.1.3 High 5900/tcp**

High (CVSS: 9.0) NVT: VNC Brute Force Login
<b>Summary</b> Try to log in with given passwords via VNC protocol.
<b>Vulnerability Detection Result</b> It was possible to connect to the VNC server with the password: password
<b>Solution</b> <b>Solution type:</b> Mitigation Change the password to something hard to guess or enable password protection at all.
... continues on next page ...

...continued from previous page...

**Vulnerability Insight**

This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all.

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

Note as well that passwords can be max. 8 characters long.

**Vulnerability Detection Method**

Details: VNC Brute Force Login

OID:1.3.6.1.4.1.25623.1.0.106056

Version used: 2019-11-06T09:58:32+0000

[\[ return to 10.0.2.4 \]](#)

**2.1.4 High 1524/tcp**

High (CVSS: 10.0)

NVT: Possible Backdoor: Ingreslock

**Summary**

A backdoor is installed on the remote host

**Vulnerability Detection Result**

The service is answering to an 'id;' command with the following response: uid=0(↩root) gid=0(root)

**Impact**

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

**Solution**

**Solution type:** Workaround

**Vulnerability Detection Method**

Details: Possible Backdoor: Ingreslock

OID:1.3.6.1.4.1.25623.1.0.103549

Version used: \$Revision: 11327 \$

[\[ return to 10.0.2.4 \]](#)

**2.1.5 High 513/tcp**

<b>High (CVSS: 7.5)</b> <b>NVT: rlogin Passwordless / Unencrypted Cleartext Login</b>
<b>Summary</b> This remote host is running a rlogin service.
<b>Vulnerability Detection Result</b> The service is misconfigured so it is allowing connections without a password.
<b>Solution</b> <b>Solution type:</b> Mitigation Disable the rlogin service and use alternatives like SSH instead.
<b>Vulnerability Insight</b> rlogin has several serious security problems, - all information, including passwords, is transmitted unencrypted. - .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password)
<b>Vulnerability Detection Method</b> Details: rlogin Passwordless / Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.901202 Version used: \$Revision: 13541 \$
<b>References</b> Other: URL: <a href="https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651">https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651</a> URL: <a href="http://en.wikipedia.org/wiki/Rlogin">http://en.wikipedia.org/wiki/Rlogin</a> URL: <a href="http://www.ietf.org/rfc/rfc1282.txt">http://www.ietf.org/rfc/rfc1282.txt</a>

[\[ return to 10.0.2.4 \]](#)

### 2.1.6 High 6667/tcp

<b>High (CVSS: 7.5)</b> <b>NVT: Check for Backdoor in UnrealIRCd</b>
<b>Summary</b> Detection of backdoor in UnrealIRCd.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Solution</b> <b>Solution type:</b> VendorFix Install latest version of unrealircd and check signatures of software you're installing.
<b>Vulnerability Insight</b> ... continues on next page ...

...continued from previous page ...
<p>Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.</p> <p>The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Details: Check for Backdoor in UnrealIRCD</p> <p>OID:1.3.6.1.4.1.25623.1.0.80111</p> <p>Version used: \$Revision: 13960 \$</p>
<p><b>References</b></p> <p>CVE: CVE-2010-2075</p> <p>BID:40820</p> <p>Other:</p> <p>URL:<a href="http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt">http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt</a></p> <p>URL:<a href="http://seclists.org/fulldisclosure/2010/Jun/277">http://seclists.org/fulldisclosure/2010/Jun/277</a></p> <p>URL:<a href="http://www.securityfocus.com/bid/40820">http://www.securityfocus.com/bid/40820</a></p>

[\[ return to 10.0.2.4 \]](#)

### 2.1.7 High 8787/tcp

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



...continued from previous page ...
↔plemented
<b>Impact</b> 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.
<b>Solution</b> <b>Solution type:</b> Mitigation Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include: - Implementing taint on untrusted input - Setting \$SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate) - Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts
<b>Vulnerability Detection Method</b> Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests. Details: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.108010 Version used: \$Revision: 12338 \$
<b>References</b> 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_testing/ ↔esters/ URL:http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html

[ [return to 10.0.2.4](#) ]

2.1.8 High general/tcp

High (CVSS: 10.0) NVT: OS End Of Life Detection
<b>Product detection result</b> cpe:/o:canonical:ubuntu_linux:8.04 Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0 ↔.105937)
... continues on next page ...

...continued from previous page ...
<b>Summary</b> OS End Of Life Detection. The Operating System on the remote host has reached the end of life and should not be used anymore.
<b>Vulnerability Detection Result</b> The "Ubuntu" Operating System on the remote host has reached the end of life. CPE: <code>cpe:/o:canonical:ubuntu_linux:8.04</code> Installed version, build or SP: 8.04 EOL date: 2013-05-09 EOL info: <a href="https://wiki.ubuntu.com/Releases">https://wiki.ubuntu.com/Releases</a>
<b>Solution</b> <b>Solution type:</b> Mitigation Upgrade the Operating System on the remote host to a version which is still supported and receiving security updates by the vendor.
<b>Vulnerability Detection Method</b> Details: OS End Of Life Detection OID:1.3.6.1.4.1.25623.1.0.103674 Version used: 2019-10-21T09:55:06+0000
<b>Product Detection Result</b> Product: <code>cpe:/o:canonical:ubuntu_linux:8.04</code> Method: OS Detection Consolidation and Reporting OID: 1.3.6.1.4.1.25623.1.0.105937)

[\[ return to 10.0.2.4 \]](#)

### 2.1.9 High 21/tcp

High (CVSS: 7.5) NVT: vsftpd Compromised Source Packages Backdoor Vulnerability
<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.
... continues on next page ...

...continued from previous page ...
<b>Solution</b> <b>Solution type:</b> VendorFix The repaired package can be downloaded from the referenced link. 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: 12076 \$
<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-backdoor.html">http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html</a> URL: <a href="https://security.appspot.com/vsftpd.html">https://security.appspot.com/vsftpd.html</a>

[\[ return to 10.0.2.4 \]](#)

### 2.1.10 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>Impact</b> DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.
<b>Solution</b> <b>Solution type:</b> VendorFix Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references.
... continues on next page ...

...continued from previous page ...

**Vulnerability Detection Method**

Details: DistCC Remote Code Execution Vulnerability

OID:1.3.6.1.4.1.25623.1.0.103553

Version used: \$Revision: 12032 \$

**References**

CVE: CVE-2004-2687

Other:

URL:https://distcc.github.io/security.html

URL:https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:  
↪80/archives/bugtraq/2005-03/0183.html[\[ return to 10.0.2.4 \]](#)**2.1.11 High 80/tcp**

High (CVSS: 10.0)

NVT: TWiki XSS and Command Execution Vulnerabilities

**Product detection result**

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

Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

**Summary**

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

**Vulnerability Detection Result**

Installed version: 01.Feb.2003

Fixed version: 4.2.4

**Impact**

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

**Solution****Solution type:** VendorFix

Upgrade to version 4.2.4 or later.

**Affected Software/OS**

TWiki, TWiki version prior to 4.2.4.

**Vulnerability Insight**

The flaws are due to,

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> <li>- %URLPARAM}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.</li> <li>- %SEARCH}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.</li> </ul>
<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: 12952 \$
<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: <a href="http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304">http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304</a> URL: <a href="http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5305">http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5305</a>

High (CVSS: 7.5)

NVT: phpinfo() output Reporting

**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 left back in the webserver directory.

**Vulnerability Detection Result**

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

<http://10.0.2.4/mutillidae/phpinfo.php>

<http://10.0.2.4/phpinfo.php>

**Impact**

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

The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

**Solution**

**Solution type:** Workaround

Delete the listed files or restrict access to them.

**Vulnerability Detection Method**

... continues on next page ...

...continued from previous page ...	
Details: phpinfo() output Reporting OID:1.3.6.1.4.1.25623.1.0.11229 Version used: \$Revision: 11992 \$	
<b>High (CVSS: 7.5)</b> <b>NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.</b>	
<b>Summary</b> PHP is prone to an information-disclosure vulnerability.	
<b>Vulnerability Detection Result</b> Vulnerable url: <a href="http://10.0.2.4/cgi-bin/php">http://10.0.2.4/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://example.com/index.php?-s">http://example.com/index.php?-s</a>	
<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: 2019-11-08T10:10:55+0000	
<b>References</b> CVE: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335 BID:53388 Other: URL: <a href="http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-risks-Update-1567532.html">http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-risks-Update-1567532.html</a> URL: <a href="http://www.kb.cert.org/vuls/id/520827">http://www.kb.cert.org/vuls/id/520827</a> URL: <a href="http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/">http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/</a> URL: <a href="https://bugs.php.net/bug.php?id=61910">https://bugs.php.net/bug.php?id=61910</a>	
... continues on next page ...	

...continued from previous page ...
URL:http://www.php.net/manual/en/security.cgi-bin.php URL:http://www.securityfocus.com/bid/53388

<b>High (CVSS: 7.5)</b> <b>NVT: Test HTTP dangerous methods</b>
<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: http://10.0.2.4/dav/puttest10774935.html We could delete the following files via the DELETE method at this web server: http://10.0.2.4/dav/puttest10774935.html
<b>Impact</b> - Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server. - Enabled DELETE method: This might allow an attacker to delete additional files on this web server.
<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: 2019-04-24T07:26:10+0000
<b>References</b> BID:12141 Other: OWASP:OWASP-CM-001

[\[ return to 10.0.2.4 \]](#)

### 2.1.12 High 512/tcp

<b>High (CVSS: 10.0)</b> <b>NVT: rexec Passwordless / Unencrypted Cleartext Login</b>
<b>Summary</b> ... continues on next page ...

...continued from previous page ...
This remote host is running a rexec service.
<b>Vulnerability Detection Result</b> The rexec service is not allowing connections from this host.
<b>Solution</b> <b>Solution type:</b> Mitigation Disable the rexec service and use alternatives like SSH instead.
<b>Vulnerability Insight</b> rexec (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 rexec authenticates by reading the username and password *unencrypted* from the socket.
<b>Vulnerability Detection Method</b> Details: rexec Passwordless / Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.100111 Version used: \$Revision: 13541 \$
<b>References</b> Other: URL: <a href="https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0618">https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0618</a>

[\[ return to 10.0.2.4 \]](#)

### 2.1.13 High 5432/tcp

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



...continued from previous page ...
<b>Vulnerability Detection Method</b> Details: PostgreSQL weak password OID:1.3.6.1.4.1.25623.1.0.103552 Version used: 2019-09-06T14:17:49+0000
<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)

[\[ return to 10.0.2.4 \]](#)

### 2.1.14 High 6200/tcp

High (CVSS: 7.5) NVT: vsftpd Compromised Source Packages Backdoor Vulnerability
<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 the referenced link. 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: 12076 \$
<b>References</b> BID:48539 Other: URL:http://www.securityfocus.com/bid/48539 URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
... continues on next page ...

...continued from previous page ...

```
↪doored.html
URL:https://security.appspot.com/vsftpd.html
```

[\[ return to 10.0.2.4 \]](#)**2.1.15 Medium 22/tcp**

Medium (CVSS: 4.3)

NVT: SSH Weak Encryption Algorithms Supported

**Summary**

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

**Vulnerability Detection Result**

The following weak client-to-server encryption algorithms are supported by the remote service:

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

The following weak server-to-client encryption algorithms are supported by the remote service:

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

**Solution**

**Solution type:** Mitigation

Disable the weak encryption algorithms.

**Vulnerability Insight**

The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

... continues on next page ...

...continued from previous page ...
<p>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.</p> <p>A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Check if remote ssh service supports Arcfour, none or CBC ciphers.</p> <p>Details: SSH Weak Encryption Algorithms Supported</p> <p>OID:1.3.6.1.4.1.25623.1.0.105611</p> <p>Version used: \$Revision: 13581 \$</p>
<p><b>References</b></p> <p>Other:</p> <p>URL:<a href="https://tools.ietf.org/html/rfc4253#section-6.3">https://tools.ietf.org/html/rfc4253#section-6.3</a></p> <p>URL:<a href="https://www.kb.cert.org/vuls/id/958563">https://www.kb.cert.org/vuls/id/958563</a></p>

[\[ return to 10.0.2.4 \]](#)

### 2.1.16 Medium 5900/tcp

<p>Medium (CVSS: 4.8)</p> <p>NVT: VNC Server Unencrypted Data Transmission</p>
<p><b>Summary</b></p> <p>The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.</p>
<p><b>Vulnerability Detection Result</b></p> <p>The VNC server provides the following insecure or cryptographically weak Security Type(s):</p> <p>2 (VNC authentication)</p>
<p><b>Impact</b></p> <p>An attacker can uncover sensitive data by sniffing traffic to the VNC server.</p>
<p><b>Solution</b></p> <p><b>Solution type:</b> Mitigation</p> <p>Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Details: VNC Server Unencrypted Data Transmission</p> <p>OID:1.3.6.1.4.1.25623.1.0.108529</p> <p>Version used: \$Revision: 13014 \$</p>
<p><b>References</b></p> <p>... continues on next page ...</p>

...continued from previous page ...

**Other:**URL: <https://tools.ietf.org/html/rfc6143#page-10>[\[ return to 10.0.2.4 \]](#)**2.1.17 Medium 445/tcp**

Medium (CVSS: 6.0)

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

**Product detection result**

cpe:/a:samba:samba:3.0.20

Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

**Summary**

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

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

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

**Solution****Solution type:** VendorFix

Updates are available. Please see the referenced vendor advisory.

**Affected Software/OS**

This issue affects Samba 3.0.0 to 3.0.25rc3.

**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: 10398 \$

**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**

... continues on next page ...

...continued from previous page ...
<b>CVE:</b> CVE-2007-2447 <b>BID:</b> 23972 <b>Other:</b> URL: <a href="http://www.securityfocus.com/bid/23972">http://www.securityfocus.com/bid/23972</a> URL: <a href="https://www.samba.org/samba/security/CVE-2007-2447.html">https://www.samba.org/samba/security/CVE-2007-2447.html</a>

[\[ return to 10.0.2.4 \]](#)

### 2.1.18 Medium 6667/tcp

<b>Medium (CVSS: 6.8)</b> <b>NVT: UnrealIRCd Authentication Spoofing Vulnerability</b>
<b>Product detection result</b> cpe:/a:unrealircd:unrealircd:3.2.8.1 Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)
<b>Summary</b> This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability.
<b>Vulnerability Detection Result</b> Installed version: 3.2.8.1 Fixed version: 3.2.10.7
<b>Impact</b> Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.
<b>Solution</b> <b>Solution type:</b> VendorFix Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.
<b>Affected Software/OS</b> UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.
<b>Vulnerability Insight</b> The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: UnrealIRCd Authentication Spoofing Vulnerability OID: 1.3.6.1.4.1.25623.1.0.809883 Version used: \$Revision: 11874 \$
<b>Product Detection Result</b> ... continues on next page ...

...continued from previous page ...
Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection OID: 1.3.6.1.4.1.25623.1.0.809884)
<b>References</b> CVE: CVE-2016-7144 BID: 92763 Other: URL: <a href="http://seclists.org/oss-sec/2016/q3/420">http://seclists.org/oss-sec/2016/q3/420</a> URL: <a href="http://www.openwall.com/lists/oss-security/2016/09/05/8">http://www.openwall.com/lists/oss-security/2016/09/05/8</a> URL: <a href="https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86bc50ba1a34a766">https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86bc50ba1a34a766</a> URL: <a href="https://bugs.unrealircd.org/main_page.php">https://bugs.unrealircd.org/main_page.php</a>

[\[ return to 10.0.2.4 \]](#)

### 2.1.19 Medium 2121/tcp

Medium (CVSS: 4.8) NVT: FTP Unencrypted Cleartext Login
<b>Summary</b> The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
<b>Vulnerability Detection Result</b> The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↵. Response(s): Anonymous sessions: 331 Password required for anonymous Non-anonymous sessions: 331 Password required for openvas-vt
<b>Impact</b> An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
<b>Solution</b> <b>Solution type:</b> Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
<b>Vulnerability Detection Method</b> Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login OID: 1.3.6.1.4.1.25623.1.0.108528
... continues on next page ...

...continued from previous page ...

Version used: \$Revision: 13611 \$

[\[ return to 10.0.2.4 \]](#)**2.1.20 Medium 25/tcp**

Medium (CVSS: 6.8)

NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability

**Summary**

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

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

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

**Solution**

**Solution type:** VendorFix

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

**Affected Software/OS**

The following vendors are affected:

Ipswitch

Kerio

Postfix

Qmail-TLS

Oracle

SCO Group

spamdyke

ISC

**Vulnerability Detection Method**

Send a special crafted 'STARTTLS' request and check the response.

Details: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection .

↪..

OID:1.3.6.1.4.1.25623.1.0.103935

Version used: \$Revision: 13204 \$

**References**

CVE: CVE-2011-0411, CVE-2011-1430, CVE-2011-1431, CVE-2011-1432, CVE-2011-1506,

... continues on next page ...

...continued from previous page...

↪CVE-2011-1575, CVE-2011-1926, CVE-2011-2165

BID:46767

Other:

URL:http://www.securityfocus.com/bid/46767

URL:http://kolab.org/pipermail/kolab-announce/2011/000101.html

URL:http://bugzilla.cyrusimap.org/show\_bug.cgi?id=3424

URL:http://cyrusimap.org/mediawiki/index.php/Bugs\_Resolved\_in\_2.4.7

URL:http://www.kb.cert.org/vuls/id/MAPG-8D9M4P

URL:http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-

↪notes.txt

URL:http://www.postfix.org/CVE-2011-0411.html

URL:http://www.pureftpd.org/project/pure-ftpd/news

URL:http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN\_ReleaseNot

↪es\_XCS\_9\_1\_1/EN\_ReleaseNotes\_WG\_XCS\_9\_1\_TLS\_Hotfix.pdf

URL:http://www.spamdyke.org/documentation/Changelog.txt

URL:http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?inclu

↪de\_text=1

URL:http://www.securityfocus.com/archive/1/516901

URL:http://support.avaya.com/css/P8/documents/100134676

URL:http://support.avaya.com/css/P8/documents/100141041

URL:http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

URL:http://inoa.net/qmail-tls/vu555316.patch

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

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

...continues on next page...



...continued from previous page ...
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436 ↔DE813CC
<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: 11103 \$

Medium (CVSS: 5.0) NVT: Check if Mailserver answer to VRFY and EXPN requests
<b>Summary</b> The Mailserver on this host answers to VRFY and/or EXPN requests.
<b>Vulnerability Detection Result</b> 'VRFY root' produces the following answer: 252 2.0.0 root
<b>Solution</b> <b>Solution type:</b> 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'. It is suggested 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.
<b>Vulnerability Insight</b> 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.
<b>Vulnerability Detection Method</b> Details: Check if Mailserver answer to VRFY and EXPN requests OID:1.3.6.1.4.1.25623.1.0.100072 Version used: \$Revision: 13470 \$
<b>References</b> Other: URL: <a href="http://cr.yp.to/smtp/vrfy.html">http://cr.yp.to/smtp/vrfy.html</a>

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 SSLv3 protocols 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: '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.
<b>Solution</b> <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.
<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: 11872 \$
<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>
... continues on next page ...

...continued from previous page ...
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.
<b>Solution</b> <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: 11402 \$
<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: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5 'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_DES40_CBC_SHA TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 TLS_RSA_EXPORT_WITH_RC4_40_MD5
<b>Impact</b> 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.
<b>Solution</b> <b>Solution type:</b> VendorFix - Remove support for 'RSA_EXPORT' cipher suites from the service. - If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.
<b>Affected Software/OS</b> - Hosts accepting 'RSA_EXPORT' cipher suites - OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.
<b>Vulnerability Insight</b> Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.
<b>Vulnerability Detection Method</b> Check previous collected cipher suites saved in the KB. Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) OID:1.3.6.1.4.1.25623.1.0.805142 Version used: 2019-07-05T09:29:25+0000
<b>References</b> CVE: CVE-2015-0204 BID:71936 Other: URL: <a href="https://freakattack.com">https://freakattack.com</a>
... continues on next page ...

...continued from previous page ...	
URL:http://secpod.org/blog/?p=3818 URL:http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-f ↳actoring-nsa.html	
Medium (CVSS: 4.0) NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	
<b>Summary</b> The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.	
<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 with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.	
<b>Vulnerability Insight</b> The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1 or fingerprint1,Fingerprint2	
<b>Vulnerability Detection Method</b> Check which hashing 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	
... continues on next page ...	

...continued from previous page...	
Version used: \$Revision: 11524 \$	
<b>References</b> Other: 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 the references). 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.	
<b>Vulnerability Detection Method</b> Checks the DHE temporary public key size. Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↪.. OID:1.3.6.1.4.1.25623.1.0.106223 Version used: \$Revision: 12865 \$	
<b>References</b> Other: URL: <a href="https://weakdh.org/">https://weakdh.org/</a> URL: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a>	

[ [return to 10.0.2.4](#) ]

## 2.1.21 Medium 21/tcp

Medium (CVSS: 6.4) NVT: Anonymous FTP Login Reporting
<b>Summary</b> Reports if the remote FTP Server allows anonymous logins.
<b>Vulnerability Detection Result</b> It was possible to login to the remote FTP service with the following anonymous ↪account(s): anonymous:anonymous@example.com ftp:anonymous@example.com
<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: - gain access to sensitive files - upload or delete files.
<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> Details: Anonymous FTP Login Reporting OID:1.3.6.1.4.1.25623.1.0.900600 Version used: \$Revision: 12030 \$
<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>

Medium (CVSS: 4.8) NVT: FTP Unencrypted Cleartext Login
<b>Summary</b> The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
... continues on next page ...



...continued from previous page ...
<b>Vulnerability Detection Result</b> The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↩. Response(s): Anonymous sessions: 331 Please specify the password. Non-anonymous sessions: 331 Please specify the password.
<b>Impact</b> An attacker can uncover login names and passwords by sniffing traffic to the FTP service.
<b>Solution</b> <b>Solution type:</b> Mitigation Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
<b>Vulnerability Detection Method</b> Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108528 Version used: \$Revision: 13611 \$

[\[ return to 10.0.2.4 \]](#)

### 2.1.22 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
<b>Impact</b> Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
... continues on next page ...

...continued from previous page ...
<b>Solution</b> <b>Solution type:</b> VendorFix Upgrade to TWiki version 4.3.2 or later.
<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: 12952 \$
<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:http://www.openwall.com/lists/oss-security/2010/08/03/8 URL:http://www.openwall.com/lists/oss-security/2010/08/02/17 URL:http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix URL:http://twiki.org/cgi-bin/view/Codev/DownloadTWiki
Medium (CVSS: 6.0) NVT: TWiki Cross-Site Request Forgery Vulnerability
<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: 4.3.1
... 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.
<b>Solution</b> <b>Solution type:</b> VendorFix Upgrade to version 4.3.1 or later.
<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: 12952 \$
<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↵ff-cve-2009-1339.txt">http://twiki.org/pub/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di↵ff-cve-2009-1339.txt</a>
Medium (CVSS: 5.8) NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled
<b>Summary</b> Debugging functions are enabled on the remote web server. The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
<b>Vulnerability Detection Result</b> The web server has the following HTTP methods enabled: TRACE
... continues on next page ...

...continued from previous page ...
<b>Impact</b> An attacker may use this flaw to trick your legitimate web users to give him their credentials.
<b>Solution</b> <b>Solution type:</b> Mitigation Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information.
<b>Affected Software/OS</b> Web servers with enabled TRACE and/or TRACK methods.
<b>Vulnerability Insight</b> It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.
<b>Vulnerability Detection Method</b> Details: HTTP Debugging Methods (TRACE/TRACK) Enabled OID:1.3.6.1.4.1.25623.1.0.11213 Version used: 2019-11-22T13:51:04+0000
<b>References</b> CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683, ↔CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE ↔-2014-7883 BID:9506, 9561, 11604, 15222, 19915, 24456, 33374, 36956, 36990, 37995 Other: URL: <a href="http://www.kb.cert.org/vuls/id/288308">http://www.kb.cert.org/vuls/id/288308</a> URL: <a href="http://www.kb.cert.org/vuls/id/867593">http://www.kb.cert.org/vuls/id/867593</a> URL: <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> URL: <a href="https://www.owasp.org/index.php/Cross_Site_Tracing">https://www.owasp.org/index.php/Cross_Site_Tracing</a>
Medium (CVSS: 5.0) NVT: /doc directory browsable
<b>Summary</b> 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.
<b>Vulnerability Detection Result</b> Vulnerable url: <a href="http://10.0.2.4/doc/">http://10.0.2.4/doc/</a>
<b>Solution</b> <b>Solution type:</b> Mitigation Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf: ... continues on next page ...

...continued from previous page ...
<Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory>
<b>Vulnerability Detection Method</b> Details: /doc directory browsable OID:1.3.6.1.4.1.25623.1.0.10056 Version used: 2019-11-22T13:51:04+0000
<b>References</b> CVE: CVE-1999-0678 BID:318

Medium (CVSS: 5.0) NVT: awiki Multiple Local File Include Vulnerabilities
<b>Summary</b> awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.
<b>Vulnerability Detection Result</b> Vulnerable url: <a href="http://10.0.2.4/mutillidae/index.php?page=/etc/passwd">http://10.0.2.4/mutillidae/index.php?page=/etc/passwd</a>
<b>Impact</b> An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host. Other attacks are also possible.
<b>Solution</b> <b>Solution type:</b> WillNotFix No known solution was made available for at least one year since the 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> awiki 20100125 is vulnerable. Other versions may also be affected.
<b>Vulnerability Detection Method</b> Details: awiki Multiple Local File Include Vulnerabilities OID:1.3.6.1.4.1.25623.1.0.103210 Version used: \$Revision: 10741 \$
<b>References</b> BID:49187 Other: URL: <a href="https://www.exploit-db.com/exploits/36047/">https://www.exploit-db.com/exploits/36047/</a> URL: <a href="http://www.securityfocus.com/bid/49187">http://www.securityfocus.com/bid/49187</a> URL: <a href="http://www.kobaonline.com/awiki/">http://www.kobaonline.com/awiki/</a>

<p>Medium (CVSS: 4.8)</p> <p>NVT: Cleartext Transmission of Sensitive Information via HTTP</p>
<p><b>Summary</b></p> <p>The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.</p>
<p><b>Vulnerability Detection Result</b></p> <p>The following input fields were identified (URL:input name):</p> <p><code>http://10.0.2.4/phpMyAdmin/:pma_password</code>  <code>http://10.0.2.4/phpMyAdmin/?D=A:pma_password</code>  <code>http://10.0.2.4/tikiwiki/tiki-install.php:pass</code>  <code>http://10.0.2.4/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword</code></p>
<p><b>Impact</b></p> <p>An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.</p>
<p><b>Solution</b></p> <p><b>Solution type:</b> Workaround</p> <p>Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.</p>
<p><b>Affected Software/OS</b></p> <p>Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.</p> <p>The script is currently checking the following:</p> <ul style="list-style-type: none"> <li>- HTTP Basic Authentication (Basic Auth)</li> <li>- HTTP Forms (e.g. Login) with input field of type 'password'</li> </ul> <p>Details: Cleartext Transmission of Sensitive Information via HTTP  OID:1.3.6.1.4.1.25623.1.0.108440  Version used: \$Revision: 10726 \$</p>
<p><b>References</b></p> <p>Other:</p> <p>URL:<a href="https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management">https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management</a></p> <p>URL:<a href="https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure">https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</a></p> <p>URL:<a href="https://cwe.mitre.org/data/definitions/319.html">https://cwe.mitre.org/data/definitions/319.html</a></p>

Medium (CVSS: 4.3) NVT: TWiki < 6.1.0 XSS Vulnerability
<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> bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.
<b>Vulnerability Detection Result</b> Installed version: 01.Feb.2003 Fixed version: 6.1.0
<b>Solution</b> <b>Solution type:</b> VendorFix Update to version 6.1.0 or later.
<b>Affected Software/OS</b> TWiki version 6.0.2 and probably prior.
<b>Vulnerability Detection Method</b> Checks if a vulnerable version is present on the target host. Details: TWiki < 6.1.0 XSS Vulnerability OID:1.3.6.1.4.1.25623.1.0.141830 Version used: 2019-03-26T08:16:24+0000
<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-2018-20212 Other: URL: <a href="https://seclists.org/fulldisclosure/2019/Jan/7">https://seclists.org/fulldisclosure/2019/Jan/7</a> URL: <a href="http://twiki.org/cgi-bin/view/Codev/DownloadTWiki">http://twiki.org/cgi-bin/view/Codev/DownloadTWiki</a>
Medium (CVSS: 4.3) NVT: phpMyAdmin 'error.php' 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 ...
<b>Summary</b> 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 inject arbitrary HTML code within the error page and conduct phishing attacks.
<b>Solution</b> <b>Solution type:</b> WillNotFix No known solution was made available for at least one year since the 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: 11553 \$
<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> ... continues on next page ...



...continued from previous page ...
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.
<b>Impact</b> Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
<b>Solution</b> <b>Solution type:</b> VendorFix Upgrade to Apache HTTP Server version 2.2.22 or later.
<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: 11857 \$
<b>References</b> CVE: CVE-2012-0053 BID:51706 Other: URL:http://secunia.com/advisories/47779 URL:http://www.exploit-db.com/exploits/18442 URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html URL:http://httpd.apache.org/security/vulnerabilities_22.html URL:http://svn.apache.org/viewvc?view=revision&revision=1235454 URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm ↔1
Medium (CVSS: 4.3) NVT: TWiki 'organization' Cross-Site Scripting Vulnerability
<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)
... continues on next page ...

...continued from previous page ...
<b>Summary</b> The host is running TWiki and is prone to cross site scripting vulnerability.
<b>Vulnerability Detection Result</b> Vulnerable url: <code>http://10.0.2.4/twiki/bin/view/Main/CccCcc</code>
<b>Impact</b> Successful exploitation will allow remote attackers to insert arbitrary HTML and script code, which will be executed in a user's browser session in the context of an affected site.
<b>Solution</b> <b>Solution type:</b> WillNotFix No known solution was made available for at least one year since the 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> TWiki version 5.1.1 and prior
<b>Vulnerability Insight</b> The flaw is due to an improper validation of user-supplied input to the 'organization' field when registering or editing a user, which allows attackers to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.
<b>Vulnerability Detection Method</b> Details: TWiki 'organization' Cross-Site Scripting Vulnerability OID:1.3.6.1.4.1.25623.1.0.802391 Version used: \$Revision: 13659 \$
<b>Product Detection Result</b> Product: <code>cpe:/a:twiki:twiki:01.Feb.2003</code> Method: TWiki Version Detection OID: 1.3.6.1.4.1.25623.1.0.800399)
<b>References</b> CVE: CVE-2012-0979 BID:51731 Other: URL: <a href="http://secunia.com/advisories/47784">http://secunia.com/advisories/47784</a> URL: <a href="http://xforce.iss.net/xforce/xfdb/72821">http://xforce.iss.net/xforce/xfdb/72821</a> URL: <a href="http://www.securitytracker.com/id?1026604">http://www.securitytracker.com/id?1026604</a> URL: <a href="http://www.securityfocus.com/bid/51731/info">http://www.securityfocus.com/bid/51731/info</a> URL: <a href="http://packetstormsecurity.org/files/109246/twiki-xss.txt">http://packetstormsecurity.org/files/109246/twiki-xss.txt</a>

[\[ return to 10.0.2.4 \]](#)

**2.1.23 Medium 23/tcp**

Medium (CVSS: 4.8) NVT: Telnet Unencrypted Cleartext Login
<b>Summary</b> The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.
<b>Solution</b> <b>Solution type:</b> Mitigation Replace Telnet with a protocol like SSH which supports encrypted connections.
<b>Vulnerability Detection Method</b> Details: Telnet Unencrypted Cleartext Login OID:1.3.6.1.4.1.25623.1.0.108522 Version used: 2019-06-06T07:39:31+0000

[\[ return to 10.0.2.4 \]](#)

**2.1.24 Medium 5432/tcp**

Medium (CVSS: 5.8) 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> 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. Please see the references for more information.
<b>Affected Software/OS</b> ... continues on next page ...

...continued from previous page ...
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: 2019-10-02T07:08:50+0000
<b>References</b> CVE: CVE-2014-0224 BID:67899 Other: URL: <a href="https://www.openssl.org/news/secadv/20140605.txt">https://www.openssl.org/news/secadv/20140605.txt</a> URL: <a href="http://www.securityfocus.com/bid/67899">http://www.securityfocus.com/bid/67899</a>

Medium (CVSS: 5.0) NVT: SSL/TLS: Certificate Expired
<b>Summary</b> The remote server's SSL/TLS certificate has already expired.
<b>Vulnerability Detection Result</b> 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
... continues on next page ...

...continued from previous page ...
<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: 11103 \$
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 proto ↪col and supports one or more ciphers. Those supported ciphers can be found in ↪the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.8 ↪02067) NVT.
<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> ... continues on next page ...

...continued from previous page ...
<p>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 \$</p>
<p><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></p>
<p>Medium (CVSS: 4.3)  NVT: SSL/TLS: Report Weak Cipher Suites</p>
<p><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.</p>
<p><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</p>
<p><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.</p>
<p><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</p>
<p><b>Vulnerability Detection Method</b>  Details: SSL/TLS: Report Weak Cipher Suites</p>
... continues on next page ...

...continued from previous page ...	
OID:1.3.6.1.4.1.25623.1.0.103440 Version used: \$Revision: 11135 \$	
<b>References</b> CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000 Other: URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16- ↪1465_update_6.html URL:https://bettercrypto.org/ URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/	
Medium (CVSS: 4.3) NVT: SSL/TLS: 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.	
<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: 11402 \$	
<b>References</b> CVE: CVE-2014-3566 BID:70574	
... continues on next page ...	

...continued from previous page ...

**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

**Summary**

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

**Vulnerability Detection Result**

The following certificates are part of the certificate chain but using insecure  
 ↪signature algorithms:

Subject: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173  
 ↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic  
 ↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi  
 ↪ng outside US,C=XX  
 Signature Algorithm: sha1WithRSAEncryption

**Solution****Solution type:** Mitigation

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

**Vulnerability Insight**

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:

Fingerprint1

or

fingerprint1,Fingerprint2

**Vulnerability Detection Method**

... continues on next page ...



...continued from previous page...	
Check which hashing 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: 11524 \$	
<b>References</b> Other: 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 the references). 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.	
<b>Vulnerability Detection Method</b> Checks the DHE temporary public key size. Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability. ↪.. OID:1.3.6.1.4.1.25623.1.0.106223 Version used: \$Revision: 12865 \$	
<b>References</b> Other: URL: <a href="https://weakdh.org/">https://weakdh.org/</a> URL: <a href="https://weakdh.org/sysadmin.html">https://weakdh.org/sysadmin.html</a>	

[\[ return to 10.0.2.4 \]](#)

### 2.1.25 Low 22/tcp

Low (CVSS: 2.6) NVT: SSH Weak MAC Algorithms Supported
<b>Summary</b> The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.
<b>Vulnerability Detection Result</b> 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
<b>Solution</b> <b>Solution type:</b> Mitigation Disable the weak MAC algorithms.
<b>Vulnerability Detection Method</b> Details: SSH Weak MAC Algorithms Supported OID:1.3.6.1.4.1.25623.1.0.105610 Version used: \$Revision: 13581 \$

[\[ return to 10.0.2.4 \]](#)

### 2.1.26 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: 353015 Packet 2: 353124 ... continues on next page ...

...continued from previous page...

**Impact**

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

**Solution****Solution type:** Mitigation

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

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

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

See the references for more information.

**Affected Software/OS**

TCP/IPv4 implementations that implement RFC1323.

**Vulnerability Insight**

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

**Vulnerability Detection Method**

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

Details: TCP timestamps

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: \$Revision: 14310 \$

**References****Other:**

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

URL:<http://www.microsoft.com/en-us/download/details.aspx?id=9152>

[\[ return to 10.0.2.4 \]](#)