# Scan Report

January 30, 2025


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 Immediate scan of IP 198.168.1.9. The scan started at Wed Jan 29 10:00:09 2025 UTC and ended at Wed Jan 21 10:38:57 2025 UTC. The report rst 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

# Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 198.168.1.9 | 19 | 35 | 2 | 0 | 0 |
| Total: 1 | 19 | 35 | 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 56 results selected by the ltering described above. Before ltering there were 384 results.

## Host Authentications

| Host | Protocol | Result | Port/User |
|---|---|---|---|
| 198.168.1.9 | SMB | Success | Protocol SMB, Port 445, User |

# Results per Host

## 198.168.1.9

Host scan start Wed Jan 29 10:00:36 2025 UTC
Host scan end Wed Jan 29 10:38:57 2025 UTC

| Service (Port) | Threat Level |
|---|---|
| 3632/tcp | High |
| 514/tcp | High |
| 22/tcp | High |
| 8787/tcp | High |
| general/tcp | High |
| 6667/tcp | High |
| 6200/tcp | High |
| 5432/tcp | High |
| 5900/tcp | High |
| 80/tcp | High |

. . . (continues) . . .

...(continued) ...

| Service (Port) | Threat Level |
|---|---|
| 513/tcp | High |
| 3306/tcp | High |
| 512/tcp | High |
| 1524/tcp | High |
| 21/tcp | High |
| 22/tcp | Medium |
| 6667/tcp | Medium |
| 5432/tcp | Medium |
| 5900/tcp | Medium |
| 80/tcp | Medium |
| 25/tcp | Medium |
| 23/tcp | Medium |
| 2121/tcp | Medium |
| 21/tcp | Medium |
| 22/tcp | Low |
| 80/tcp | Low |

## High 3632/tcp

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

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

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

### 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: VendorFix
Vendor updates are available. Please see the references for more information.
For more information about DistCC's security see the references.

### Vulnerability Detection Method
Details: `DistCC Remote Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103553
Version used: `$Revision: 12032 $`

...continues on next page ...

... continued from previous page ...

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 198.168.1.9 ]

## High 514/tcp

High (CVSS: 7.5)
NVT: rsh Unencrypted Cleartext Login

Summary
This remote host is running a rsh service.

Vulnerability Detection Result
The rsh service is misconfigured so it is allowing conntections without a passwo
↪rd or with default root:root credentials.

Solution
Solution type: Mitigation
Disable the rsh service and use alternatives like SSH instead.

Vulnerability Insight
rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network.

Vulnerability Detection Method
Details: rsh Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.100080
Version used: $Revision: 13010 $

References
Other:
URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651

[ return to 198.168.1.9 ]

## High 22/tcp

| High (CVSS: 7.5)<br>NVT: SSH Brute Force Logins With Default Credentials Reporting |
|---|
| Summary<br>It was possible to login into the remote SSH server using default credentials.<br>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 vulner- ability takes place in this NVT instead. The script preference 'Report timeout' allows you to con gure if such an timeout is reported. |
| Vulnerability Detection Result<br>It was possible to login with the following credentials <User>:<Password><br>msfadmin:msfadmin<br>user:user |
| Solution<br>Solution type: Mitigation<br>Change the password as soon as possible. |
| Vulnerability Detection Method<br>Try to login with a number of known default credentials via the SSH protocol.<br>Details: SSH Brute Force Logins With Default Credentials Reporting<br>OID:1.3.6.1.4.1.25623.1.0.103239<br>Version used: $Revision: 13568 $ |

[ return to 198.168.1.9 ]

High 8787/tcp

| High (CVSS: 10.0)<br>NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities |
|---|
| Summary<br>Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands. |
| Vulnerability Detection Result<br>The service is running in $SAFE >= 1 mode. However it is still possible to run a<br>‹→rbitrary syscall commands on the remote host. Sending an invalid syscall the s<br>‹→ervice returned the following response:<br>Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in `syscall'"0/usr/lib/<br>‹→ruby/1.8/drb/drb.rb:1555:in `send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in `__se<br>‹→nd__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in `perform_without_block'"3/usr/lib/<br>‹→ruby/1.8/drb/drb.rb:1515:in `perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in `m<br>‹→ain_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in `loop'"5/usr/lib/ruby/1.8/drb/<br>‹→drb.rb:1585:in `main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in `start'"5/usr<br>‹→/lib/ruby/1.8/drb/drb.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:143 |
| ... continues on next page ... |

... continued from previous page ...

‹→0:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in `start'"//usr/lib/ruby/1.8/dr
‹→b/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize'"//us
‹→r/lib/ruby/1.8/drb/drb.rb:1627:in `new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
‹→`start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
‹→plemented

Impact
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.

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

Vulnerability Detection Method
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 $

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

[ return to 198.168.1.9 ]

## High general/tcp

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

Product detection result

... continues on next page ...

... continued from previous page ...

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)

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

Vulnerability Detection Result
The "Ubuntu" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP: 8.04
EOL date: 2013-05-09
EOL info: https://wiki.ubuntu.com/Releases

Solution
Solution type: Mitigation

Vulnerability Detection Method
Details: OS End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: $Revision: 8927 $

Product Detection Result
Product: cpe:/o:canonical:ubuntu_linux:8.04
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[ return to 198.168.1.9 ]

## High 6667/tcp

High (CVSS: 7.5)
NVT: Check for Backdoor in UnrealIRCd

Summary
Detection of backdoor in UnrealIRCd.

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

Solution
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Install latest version of unrealircd and check signatures of software you're installing.

Vulnerability Insight
Remote attackers can exploit this issue to execute arbitrary system commands within the context of the a ected application.
The issue a ects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz down- loaded in November 2009 and later is a ected. The MD5 sum of the a ected le is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not a ected.

Vulnerability Detection Method
Details: Check for Backdoor in UnrealIRCd
OID:1.3.6.1.4.1.25623.1.0.80111
Version used: $Revision: 13960 $

References
CVE: CVE-2010-2075
BID:40820
Other:
URL:http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt
URL:http://seclists.org/fulldisclosure/2010/Jun/277
URL:http://www.securityfocus.com/bid/40820

[ return to 198.168.1.9 ]

## High 6200/tcp

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

Summary
vsftpd is prone to a backdoor vulnerability.

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

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

Solution
Solution type: VendorFix
The repaired package can be downloaded from the referenced link. Please validate the package with its signature.

A ected Software/OS

... continues on next page ...

... continued from previous page ...

The vsftpd 2.3.4 source package is a ected.

Vulnerability Detection Method
Details: vsftpd Compromised Source Packages Backdoor Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: $Revision: 12076 $

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

[ return to 198.168.1.9 ]

## High 5432/tcp

High (CVSS: 9.0)
NVT: PostgreSQL weak password

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

Summary
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Vulnerability Detection Result
It was possible to login as user postgres with password "postgres".

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

Vulnerability Detection Method
Details: PostgreSQL weak password
OID:1.3.6.1.4.1.25623.1.0.103552
Version used: $Revision: 10312 $

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)

[ return to 198.168.1.9 ]

## High 5900/tcp

| High (CVSS: 9.0)<br>NVT: VNC Brute Force Login |
|---|
| Summary<br>Try to log in with given passwords via VNC protocol. |
| Vulnerability Detection Result<br>It was possible to connect to the VNC server with the password: password |
| Solution<br>Solution type: Mitigation<br>Change the password to something hard to guess or enable password protection at all. |
| Vulnerability Insight<br>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.<br>Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after ve unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked.<br>Note as well that passwords can be max. 8 characters long. |
| Vulnerability Detection Method<br>Details: VNC Brute Force Login<br>OID:1.3.6.1.4.1.25623.1.0.106056<br>Version used: $Revision: 13328 $ |

[ return to 198.168.1.9 ]

## High 80/tcp

| High (CVSS: 10.0)<br>NVT: TWiki XSS and Command Execution Vulnerabilities |
|---|
| Product detection result<br>cpe:/a:twiki:twiki:01.Feb.2003<br>Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399) |
| Summary<br>The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities. |

. . . continues on next page . . .

... continued from previous page ...

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 a ected application.

Solution
Solution type: VendorFix
Upgrade to version 4.2.4 or later.

A ected Software/OS
TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight
The aws are due to,
- %URLPARAM}}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.
- %SEARCH}}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details: TWiki XSS and Command Execution Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: $Revision: 12952 $

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

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

High (CVSS: 7.5)
NVT: Tiki Wiki CMS Groupware < 4.2 Multiple Unspeci ed Vulnerabilities

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

... continues on next page ...

... continued from previous page ...

‹→0.901001)

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

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 4.2

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

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

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

Vulnerability Detection Method
Details: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100537
Version used: $Revision: 13960 $

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

References
CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136
BID:38608
Other:
URL:http://www.securityfocus.com/bid/38608
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=247
‹→34
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=250
‹→46
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254
‹→24

... continues on next page ...

... continued from previous page ...

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

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

Summary
Many PHP installation tutorials instruct the user to create a le called phpinfo.php or similar containing the phpinfo() statement. Such a le 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:// 198.168.1.9/mutillidae/phpinfo.php
http:// 198.168.1.9/phpinfo.php

Impact
Some of the information that can be gathered from this le 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 les or restrict access to them.

Vulnerability Detection Method
Details: phpinfo() output Reporting
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: $Revision: 11992 $

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

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result
Vulnerable url: http:// 198.168.1.9/cgi-bin/php

Impact

... continues on next page ...

... continued from previous page ...

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

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

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

Vulnerability Detection Method
Details: PHP-CGI-based setups vulnerability when parsing query string parameters fr m ph.
‹→..
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: $Revision: 13679 $

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

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

Summary
Miscon gured 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 les.

Vulnerability Detection Result
We could upload the following files via the PUT method at this web server:
http://198.168.1.9/dav/puttest1805774771.html

... continues on next page ...

... continued from previous page ...

We could delete the following files via the DELETE method at this web server:
http://198.168.1.9/dav/puttest1805774771.html

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

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

Vulnerability Detection Method
Details: Test HTTP dangerous methods
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: $Revision: 9335 $

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

[ return to 198.168.1.9 ]

## High 513/tcp

High (CVSS: 7.5)
NVT: rlogin Passwordless / Unencrypted Cleartext Login

Summary
This remote host is running a rlogin service.

Vulnerability Detection Result
The service is misconfigured so it is allowing conntections without a password.

Solution
Solution type: Mitigation
Disable the rlogin service and use alternatives like SSH instead.

Vulnerability Insight
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)

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details: rlogin Passwordless / Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.901202
Version used: $Revision: 13541 $

References
Other:
URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651
URL:http://en.wikipedia.org/wiki/Rlogin
URL:http://www.ietf.org/rfc/rfc1282.txt

[ return to 198.168.1.9 ]

## High 3306/tcp

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

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

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

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

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

Vulnerability Detection Method
Details: MySQL / MariaDB weak password
OID:1.3.6.1.4.1.25623.1.0.103551
Version used: $Revision: 12175 $

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

[ return to 198.168.1.9 ]

## High 512/tcp

| High (CVSS: 10.0)<br>NVT: rexec Passwordless / Unencrypted Cleartext Login |
|---|
| Summary<br>This remote host is running a rexec service. |
| Vulnerability Detection Result<br>The rexec service is not allowing connections from this host. |
| Solution<br>Solution type: Mitigation<br>Disable the rexec service and use alternatives like SSH instead. |
| Vulnerability Insight<br>rexec (Remote Process Execution) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.<br>The main di erence is that rexec authenticate by reading the username and password *unencrypted* from the socket. |
| Vulnerability Detection Method<br>Details: rexec Passwordless / Unencrypted Cleartext Login<br>OID:1.3.6.1.4.1.25623.1.0.100111<br>Version used: $Revision: 13541 $ |
| References<br>Other:<br>URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0618 |

[ return to 198.168.1.9 ]

## High 1524/tcp

| High (CVSS: 10.0)<br>NVT: Possible Backdoor: Ingreslock |
|---|
| Summary<br>A backdoor is installed on the remote host |
| Vulnerability Detection Result<br>The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root) |
| Impact<br>Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the a ected isystem. |
| Solution |

. . . continues on next page . . .

... continued from previous page ...

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 198.168.1.9 ]

## High 21/tcp

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

Summary
vsftpd is prone to a backdoor vulnerability.

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

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

Solution
Solution type: VendorFix
The repaired package can be downloaded from the referenced link. Please validate the package with its signature.

A ected Software/OS
The vsftpd 2.3.4 source package is a ected.

Vulnerability Detection Method
Details: vsftpd Compromised Source Packages Backdoor Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: $Revision: 12076 $

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

[ return to 198.168.1.9 ]

## Medium 22/tcp

| Medium (CVSS: 4.3)<br>NVT: SSH Weak Encryption Algorithms Supported |
|---|
| Summary<br>The remote SSH server is con gured to allow weak encryption algorithms. |
| Vulnerability Detection Result<br>The following weak client-to-server encryption algorithms are supported by the r<br>‹→emote service:<br>3des-cbc<br>aes128-cbc<br>aes192-cbc<br>aes256-cbc<br>arcfour<br>arcfour128<br>arcfour256<br>blowfish-cbc<br>cast128-cbc<br>rijndael-cbc@lysator.liu.se<br>The following weak server-to-client encryption algorithms are supported by the r<br>‹→emote service:<br>3des-cbc<br>aes128-cbc<br>aes192-cbc<br>aes256-cbc<br>arcfour<br>arcfour128<br>arcfour256<br>blowfish-cbc<br>cast128-cbc<br>rijndael-cbc@lysator.liu.se |
| Solution<br>Solution type: Mitigation<br>Disable the weak encryption algorithms. |
| Vulnerability Insight<br>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.<br>The `none` algorithm speci es that no encryption is to be done. Note that this method provides no con dentiality protection, and it is NOT RECOMMENDED to use it.<br>A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext. |
| Vulnerability Detection Method |
| . . . continues on next page . . . |

... continued from previous page ...

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: 13581 $

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

[ return to 198.168.1.9 ]

## Medium 6667/tcp

Medium (CVSS: 6.8)
NVT: UnrealIRCd Authentication Spoo ng Vulnerability

Product detection result
cpe:/a:unrealircd:unrealircd:3.2.8.1
Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)

Summary
This host is installed with UnrealIRCd and is prone to authentication spoo ng vulnerability.

Vulnerability Detection Result
Installed version: 3.2.8.1
Fixed version: 3.2.10.7

Impact
Successful exploitation of this vulnerability will allows remote attackers to spoof certi cate n-gerprints and consequently log in as another user.

Solution
Solution type: VendorFix
Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.

A ected Software/OS
UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.

Vulnerability Insight
The aw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: UnrealIRCd Authentication Spoofing Vulnerability

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.809883
Version used: $Revision: 11874 $

Product Detection Result
Product: cpe:/a:unrealircd:unrealircd:3.2.8.1
Method: UnrealIRCd Detection
OID: 1.3.6.1.4.1.25623.1.0.809884)

References
CVE: CVE-2016-7144
BID:92763
Other:
URL:http://seclists.org/oss-sec/2016/q3/420
URL:http://www.openwall.com/lists/oss-security/2016/09/05/8
URL:https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf8
↪6bc50ba1a34a766
URL:https://bugs.unrealircd.org/main_page.php

[ return to 198.168.1.9 ]

## Medium 5432/tcp

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

Summary
OpenSSL is prone to security-bypass vulnerability.

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

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

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

A ected Software/OS
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Method
Send two SSL ChangeCipherSpec request and check the response.
Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105042
Version used: $Revision: 12865 $

References
CVE: CVE-2014-0224
BID:67899
Other:
URL:https://www.openssl.org/news/secadv/20140605.txt
URL:http://www.securityfocus.com/bid/67899
URL:http://openssl.org/

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certi cate Expired

Summary
The remote server's SSL/TLS certi cate 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

... continues on next page ...

... continued from previous page ...

Replace the SSL/TLS certi cate by a new one.

Vulnerability Insight
This script checks expiry dates of certi cates 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: 11103 $

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

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

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

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

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

A ected Software/OS
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

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

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

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 5547 $

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

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

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

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

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

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

Vulnerability Detection Method
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: $Revision: 11135 $

... continues on next page ...

... continued from previous page ...

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

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

Summary
This host is prone to an information disclosure vulnerability.

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

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

Solution
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

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

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ...
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: $Revision: 11402 $

References
CVE: CVE-2014-3566
BID:70574
Other:
URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
URL:https://www.imperialviolet.org/2014/10/14/poodle.html

... continues on next page ...

... continued from previous page ...

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: Certi cate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certi cate in the certi cate 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 certi cates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certi cates to avoid web browser SSL/TLS certi cate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certi cates 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) certi cates.
NOTE: The script preference allows to set one or more custom SHA-1 ngerprints of CA certi - cates which are trusted by this routine. The ngerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
ngerprint1,Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certi cate.
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 $

References
Other:
URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Medium (CVSS: 4.0)
NVT: SSL/TLS: Di e-Hellman Key Exchange Insu cient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Di e-Hellman groups with insu cient strength (key size < 2048).

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits

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

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Di e-Hellman (ECDHE) or use a 2048-bit or stronger Di e-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.

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

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnera bili.
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: $Revision: 12865 $

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

[ return to 198.168.1.9 ]

## Medium 5900/tcp

| Medium (CVSS: 4.8)<br>NVT: VNC Server Unencrypted Data Transmission |
|---|
| Summary<br>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. |
| Vulnerability Detection Result<br>The VNC server provides the following insecure or cryptographically weak Securit<br>↪y Type(s):<br>2 (VNC authentication) |
| Impact<br>An attacker can uncover sensitive data by sni ng tra c to the VNC server. |
| Solution<br>Solution type: Mitigation<br>Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254].<br>Some VNC server vendors are also providing more secure Security Types within their products. |
| Vulnerability Detection Method<br>Details: VNC Server Unencrypted Data Transmission<br>OID:1.3.6.1.4.1.25623.1.0.108529<br>Version used: $Revision: 13014 $ |
| References<br>Other:<br>URL:https://tools.ietf.org/html/rfc6143#page-10 |

[ return to 198.168.1.9]

## Medium 80/tcp

| Medium (CVSS: 6.8)<br>NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10 |
|---|
| Product detection result<br>cpe:/a:twiki:twiki:01.Feb.2003<br>Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399) |
| Summary<br>The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability. |

. . . continues on next page . . .

... continued from previous page ...

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

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

Solution
Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later.

A ected Software/OS
TWiki version prior to 4.3.2

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

Vulnerability Detection Method
Details: TWiki Cross-Site Request Forgery Vulnerability - Sep10
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: $Revision: 12952 $

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

References
CVE: CVE-2009-4898
Other:
URL:http://www.openwall.com/lists/oss-security/2010/08/03/8
URL:http://www.openwall.com/lists/oss-security/2010/08/02/17
URL:http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix
URL:http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Medium (CVSS: 6.5)
NVT: Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability

Product detection result
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
‹→0.901001)
... continues on next page ...

. . . continued from previous page . . .

Summary
In Tiki the user task component is vulnerable to a SQL Injection via the tiki-user_tasks.php show_history parameter.

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 17.2

Solution
Solution type: VendorFix
Upgrade to version 17.2 or later.

A ected Software/OS
Tiki Wiki CMS Groupware prior to version 17.2.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141885
Version used: $Revision: 13115 $

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

References
CVE: CVE-2018-20719
Other:
URL:https://blog.ripstech.com/2018/scan-verify-patch-security-issues-in-minute
↪s/

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

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

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

. . . continues on next page . . .

... continued from previous page ...

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

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

Solution
Solution type: VendorFix
Upgrade to version 4.3.1 or later.

A ected Software/OS
TWiki version prior to 4.3.1

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

Vulnerability Detection Method
Details: TWiki Cross-Site Request Forgery Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: $Revision: 12952 $

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

References
CVE: CVE-2009-1339
Other:
URL:http://secunia.com/advisories/34880
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258
URL:http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di
↪ff-cve-2009-1339.txt

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
The web server has the following HTTP methods enabled: TRACE

Impact
An attacker may use this aw to trick your legitimate web users to give him their credentials.

Solution
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server con guration.
Please see the manual of your web server or the references for more information.

A ected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
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.

Vulnerability Detection Method
Details: HTTP Debugging Methods (TRACE/TRACK) Enabled
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: $Revision: 10828 $

References
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:http://www.kb.cert.org/vuls/id/288308
URL:http://www.kb.cert.org/vuls/id/867593
URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
URL:https://www.owasp.org/index.php/Cross_Site_Tracing

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

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

Summary
... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 2.2

Impact
Successful exploitation could allow arbitrary code execution in the context of an a ected site.

Solution
Solution type: VendorFix
Upgrade to version 2.2 or later.

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

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

Vulnerability Detection Method
Details: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800315
Version used: $Revision: 14010 $

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

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

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

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

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerable url: http:// 198.168.1.9/doc/

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

Vulnerability Detection Method
Details: /doc directory browsable
OID:1.3.6.1.4.1.25623.1.0.10056
Version used: $Revision: 14336 $

References
CVE: CVE-1999-0678
BID:318

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

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

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

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 12.11

Impact
Successful exploitation will allow an user having access to the admin backend to gain access to arbitrary les and to compromise the application.

Solution
Solution type: VendorFix
Upgrade to Tiki Wiki CMS Groupware version 12.11 LTS, 15.4 or later.

A ected Software/OS
Tiki Wiki CMS Groupware versions:
- below 12.11 LTS

... continues on next page ...

... continued from previous page ...

- 13.x, 14.x and 15.x below 15.4

Vulnerability Insight
The Flaw is due to improper sanitization of input passed to the 'xedURLData' parameter of the 'display_banner.php' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability
OID:1.3.6.1.4.1.25623.1.0.108064
Version used: $Revision: 11863 $

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

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

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

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

Vulnerability Detection Result
Vulnerable url: http:// 198.168.1.9/mutillidae/index.php?page=/etc/passwd

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

Solution
Solution type: WillNotFix
No 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.

... continues on next page ...

... continued from previous page ...

A ected Software/OS
awiki 20100125 is vulnerable. Other versions may also be a ected.

Vulnerability Detection Method
Details: awiki Multiple Local File Include Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.103210
Version used: $Revision: 10741 $

References
BID:49187
Other:
URL:https://www.exploit-db.com/exploits/36047/
URL:http://www.securityfocus.com/bid/49187
URL:http://www.kobaonline.com/awiki/

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
The following input fields where identified (URL:input name):
http:// 198.168.1.9/phpMyAdmin/:pma_password
http:// 198.168.1.9/phpMyAdmin/?D=A:pma_password
http:// 198.168.1.9/tikiwiki/tiki-install.php:pass
http://198.168.1.9/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword

Impact
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.

Solution
Solution type: Workaround
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.

A ected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: $Revision: 10726 $

References
Other:
URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
‹→ession_Management
URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
URL:https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 4.3)
NVT: TWiki < 6.1.0 XSS Vulnerability

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

Summary
bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 6.1.0

Solution
Solution type: VendorFix
Update to version 6.1.0 or later.

A ected Software/OS
TWiki version 6.0.2 and probably prior.

Vulnerability Detection Method
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

Product Detection Result
Product: cpe:/a:twiki:twiki:01.Feb.2003

... continues on next page ...

... continued from previous page ...

Method: TWiki Version Detection
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
CVE: CVE-2018-20212
Other:
URL:https://seclists.org/fulldisclosure/2019/Jan/7
URL:http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

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

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

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

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

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

Solution
Solution type: 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.

A ected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

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

Vulnerability Detection Method
Details: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: $Revision: 11553 $

... continues on next page ...

... continued from previous page ...

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

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

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

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

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

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

Solution
Solution type: VendorFix
Upgrade to Apache HTTP Server version 2.2.22 or later.

A ected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21

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

Vulnerability Detection Method
Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: $Revision: 11857 $

References
CVE: CVE-2012-0053
BID:51706

... continues on next page ...

... continued from previous page ...

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

[ return to 198.168.1.9 ]

## 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.

### A ected Software/OS
The following vendors are a ected:
Ipswitch
Kerio
Post x
Qmail-TLS
Oracle
SCO Group
spamdyke
ISC

### Vulnerability Detection Method
Send a special crafted 'STARTTLS' request and check the response.

... continues on next page ...

... continued from previous page ...

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, ↪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: Check if Mailserver answer to VRFY and EXPN requests

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

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 post x add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.

... continues on next page ...

... continued from previous page ...

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.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through rewalls, gateways, mail exchangers for part-time hosts, etc.

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: 13470 $

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

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certi cate Expired

Summary
The remote server's SSL/TLS certi cate 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 certi cate by a new one.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

This script checks expiry dates of certi cates 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: 11103 $

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

Summary
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

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

Impact
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are signi cantly 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.

Solution
Solution type: 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.

A ected Software/OS
- 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.

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

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: $Revision: 11872 $

References
CVE: CVE-2015-0204
BID:71936
Other:
URL:https://freakattack.com
URL:http://secpod.org/blog/?p=3818
URL:http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-f
↩actoring-nsa.html
URL:https://www.openssl.org

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

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

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

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

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

A ected Software/OS
All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Check the used protocols of the services provided by this system.
Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: $Revision: 5547 $

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

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

Summary
This host is prone to an information disclosure vulnerability.

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

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

Solution
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

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

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

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 11402 $

References
CVE: CVE-2014-3566
BID:70574
Other:
URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
URL:https://www.imperialviolet.org/2014/10/14/poodle.html
URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit
↪ing-ssl-30.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

Summary
This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.

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

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

Solution
Solution type: VendorFix
- Remove support for 'DHE_EXPORT' cipher suites from the service
- If running OpenSSL updateto version 1.0.2b or 1.0.1n or later.

A ected Software/OS
- Hosts accepting 'DHE_EXPORT' cipher suites
- OpenSSL version before 1.0.2b and 1.0.1n

Vulnerability Insight
Flaw is triggered when handling Di e-Hellman key exchanges de ned in the 'DHE_EXPORT' cipher suites.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (Log jam)
OID:1.3.6.1.4.1.25623.1.0.805188
Version used: $Revision: 11872 $

References
CVE: CVE-2015-4000
BID:74733
Other:
URL:https://weakdh.org
URL:https://weakdh.org/imperfect-forward-secrecy.pdf
URL:http://openwall.com/lists/oss-security/2015/05/20/8
URL:https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained
URL:https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-change
↪s

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certi cate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certi cate in the certi cate 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 certi cates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certi cates to avoid web browser SSL/TLS certi cate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certi cates 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)

... continues on next page ...

... continued from previous page ...

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) certi cates.
NOTE: The script preference allows to set one or more custom SHA-1 ngerprints of CA certi - cates which are trusted by this routine. The ngerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
ngerprint1,Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certi cate.
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 $

References
Other:
URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Medium (CVSS: 4.0)
NVT: SSL/TLS: Di e-Hellman Key Exchange Insu cient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Di e-Hellman groups with insu cient strength (key size < 2048).

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits

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

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Di e-Hellman (ECDHE) or use a 2048-bit or stronger Di e-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.

Vulnerability Insight
The Di e-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, xed. The security of the nal 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 ...

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnera bili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: $Revision: 12865 $

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

[ return to 198.168.1.9 ]

## Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

Summary
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

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

Impact
An attacker can uncover login names and passwords by sni ng tra c to the Telnet service.

Solution
Solution type: Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method
Details: Telnet Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108522
Version used: $Revision: 13620 $

[ return to 198.168.1.9 ]

## Medium 2121/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

... continues on next page ...

... continued from previous page ...

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result
```
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
```

Impact
An attacker can uncover login names and passwords by sni ng tra c to the FTP service.

Solution
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command rst 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 198.168.1.9 ]

## Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Anonymous FTP Login Reporting

Summary
Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result
```
It was possible to login to the remote FTP service with the following anonymous
↪account(s):
anonymous:anonymous@example.com
ftp:anonymous@example.com
```

Impact
Based on the les accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
- gain access to sensitive les

... continues on next page ...

... continued from previous page ...

- upload or delete les.

Solution
Solution type: Mitigation
If you do not want to share les, you should disable anonymous logins.

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

Vulnerability Detection Method
Details: Anonymous FTP Login Reporting
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: $Revision: 12030 $

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

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result
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.

Impact
An attacker can uncover login names and passwords by sni ng tra c to the FTP service.

Solution
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command rst and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

... continues on next page ...

... continued from previous page ...

Details: FTP Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: $Revision: 13611 $

[ return to 198.168.1.9 ]

## Low 22/tcp

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

**Summary**
The remote SSH server is con gured 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: 13581 $

[ return to 198.168.1.9 ]

## Low 80/tcp

### Low (CVSS: 3.5)
### NVT: Tiki Wiki CMS Groupware XSS Vulnerability

**Product detection result**
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5

... continues on next page ...

... continued from previous page ...

Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)

Summary
An XSS vulnerability (via an SVG image) in Tiki allows an authenticated user to gain administrator privileges if an administrator opens a wiki page with a malicious SVG image, related to lib/ legals/ legallib.php.

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 18.0

Solution
Solution type: VendorFix
Upgrade to version 18.0 or later.

A ected Software/OS
Tiki Wiki CMS Groupware prior to version 18.0.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Tiki Wiki CMS Groupware XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.140797
Version used: $Revision: 12116 $

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

References
CVE: CVE-2018-7188
Other:
URL:http://openwall.com/lists/oss-security/2018/02/16/1

[ return to 198.168.1.9 ]