# Summary

This document reports on the results of an automatic security scan. 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.

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 39 results selected by the filtering described above. Before filtering there were 326 results.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

| | |
|---|---|
| Scan started: | **Fri Oct 24 20:25:54 2021 UTC** |
| Scan ended: | Fri Oct 24 20:51:56 2021 UTC |
| Task: | METASPLOITABLE |

## Host Summary

| Host | Start | End | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|---|---|
| 192.168.1.98 | Oct 24, 20:25:54 | Oct 24, 20:51:56 | 9 | 28 | 2 | 0 | 0 |
| Total: 1 | | | 9 | 28 | 2 | 0 | 0 |

## Host Authentications

| Host | Protocol | Result | Port/User |
|---|---|---|---|
| 192.168.1.98 | SMB | Success | Protocol SMB, Port 445, User |

# Results per Host

## Host 192.168.1.98

| | |
|---|---|
| Scanning of this host started at: | Sun Feb 21 18:20:54 2021 UTC |
| Number of results: | 39 |

### Port Summary for Host 192.168.1.98

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 5432/tcp | High |
| 22/tcp | High |
| 25/tcp | Medium |
| 3306/tcp | High |
| general/tcp | High |
| 23/tcp | Medium |
| 3632/tcp | High |

## Security Issues for Host 192.168.1.98

**High** (CVSS: 10.0) general/tcp
NVT: OS End Of Life Detection (OID: 1.3.6.1.4.1.25623.1.0.103674)

Product detection result: cpe:/o:canonical:ubuntu_linux:8.04 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)

**High** (CVSS: 10.0) 80/tcp
NVT: TWiki XSS and Command Execution Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.800320)

Product detection result: cpe:/a:twiki:twiki:01.Feb.2003 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,

- %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: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304
http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305

**High** (CVSS: 9.3) 3632/tcp
NVT: DistCC Remote Code Execution Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103553)

**Summary**

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

**Vulnerability Detection Result**

```
It was possible to execute the "id" command.

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

**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 $

**References**

CVE: CVE-2004-2687
CERT: DFN-CERT-2019-0381
Other: https://distcc.github.io/security.html
https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80/archives/bugtraq/2005-03/0183.html

**High** (CVSS: 9.0) 3306/tcp
NVT: MySQL / MariaDB weak password (OID: 1.3.6.1.4.1.25623.1.0.103551)

Product detection result: cpe:/a:mysql:mysql:5.0.51a 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 password "root".
```

**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)

**High** (CVSS: 9.0) 5432/tcp
NVT: PostgreSQL weak password (OID: 1.3.6.1.4.1.25623.1.0.103552)

Product detection result: cpe:/a:postgresql:postgresql:8.3.1 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)

**High** (CVSS: 7.8) 80/tcp
NVT: Apache httpd Web Server Range Header Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.901203)

**Summary**

This host is running Apache httpd web server and is prone to denial of service vulnerability.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

Successful exploitation will let the remote unauthenticated attackers to cause a denial of service.

**Solution**

**Solution type:** Mitigation

Please see the references for a fix to mitigate this issue.

**Affected Software/OS**

Apache 1.3.x, 2.0.x through 2.0.64 and 2.2.x through 2.2.19.

**Vulnerability Insight**

The flaw is caused the way Apache httpd web server handles certain requests with multiple overlapping ranges, which causes significant memory and CPU usage on the server leading to application crash and system can become unstable.

**Vulnerability Detection Method**

Details: Apache httpd Web Server Range Header Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.901203)

Version used: $Revision: 13659 $

**References**

CVE: CVE-2011-3192
BID: 49303
CERT: DFN-CERT-2012-1112, DFN-CERT-2012-0856, DFN-CERT-2012-0746, DFN-CERT-2012-0731, DFN-CERT-2011-1726, DFN-CERT-2011-1725, DFN-CERT-2011-1693, DFN-CERT-2011-1692, DFN-CERT-2011-1632, DFN-CERT-2011-1631, DFN-CERT-2011-1593, DFN-CERT-2011-1519, DFN-CERT-2011-1492, DFN-CERT-2011-1440, DFN-CERT-2011-1435, DFN-CERT-2011-1430, DFN-CERT-2011-1429, DFN-CERT-2011-1425, DFN-CERT-2011-1379, DFN-CERT-2011-1362, DFN-CERT-2011-1343, DFN-CERT-2011-1342, DFN-CERT-2011-1341, DFN-CERT-2011-1335, DFN-CERT-2011-1333, DFN-CERT-2011-1318, DFN-CERT-2011-1312, DFN-CERT-2011-1298
Other: http://www.exploit-db.com/exploits/17696
http://packetstormsecurity.org/files/view/104441
http://marc.info/?l=apache-httpd-dev&m=131420013520206&w=2

http://mail-archives.apache.org/mod_mbox/httpd-dev/201108.mbox/%3CCAAPSnn2PO-d-C4nQt_TES2RRWiZr7urefhTKPWBC1b+K1Dqc7g@mail.gmail.com%3E

**High** (CVSS: 7.5) 80/tcp

NVT: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.100537)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

**Summary**

Tiki Wiki CMS Groupware is prone to multiple unspecified vulnerabilities, including:

- An unspecified SQL-injection vulnerability

- An unspecified authentication-bypass vulnerability

- An unspecified vulnerability

**Vulnerability Detection Result**

```
Installed version: 1.9.5
Fixed version:     4.2
```

**Impact**

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

**Solution**

**Solution type:** VendorFix

The vendor has released an advisory and fixes. Please see the references for details.

**Affected Software/OS**

Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.

**Vulnerability Detection Method**

Details: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.100537)

Version used: $Revision: 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: http://www.securityfocus.com/bid/38608
http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=24734
http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25046
http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25424
http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25435
http://info.tikiwiki.org/article86-Tiki-Announces-3-5-and-4-2-Releases
http://info.tikiwiki.org/tiki-index.php?page=homepage

**High** (CVSS: 7.5) 80/tcp
NVT: phpinfo() output Reporting (OID: 1.3.6.1.4.1.25623.1.0.11229)

**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 potentially sensitive information:

http://192.168.1.98/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**

Details: phpinfo() output Reporting (OID: 1.3.6.1.4.1.25623.1.0.11229)

Version used: $Revision: 11992 $

**High** (CVSS: 7.5) 22/tcp
NVT: SSH Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103239)

**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: $Revision: 13568 $

**Medium** (CVSS: 6.8) 80/tcp
NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10 (OID: 1.3.6.1.4.1.25623.1.0.801281)

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

**Summary**

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

**Vulnerability Detection Result**

```
Installed version: 01.Feb.2003
Fixed version:     4.3.2
```

**Impact**

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

**Solution**

**Solution type:** VendorFix

Upgrade to TWiki version 4.3.2 or later.

**Affected Software/OS**

TWiki version prior to 4.3.2

**Vulnerability Insight**

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

**Vulnerability Detection Method**

Details: TWiki Cross-Site Request Forgery Vulnerability - Sep10 (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: http://www.openwall.com/lists/oss-security/2010/08/03/8
http://www.openwall.com/lists/oss-security/2010/08/02/17
http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix
http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

**Medium** (CVSS: 6.8) 25/tcp
NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection ... (OID: 1.3.6.1.4.1.25623.1.0.103935)

**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, CVE-2011-1575, CVE-2011-1926, CVE-2011-2165

BID: 46767

CERT: CB-K15/1514, DFN-CERT-2011-0917, DFN-CERT-2011-0912, DFN-CERT-2011-0897, DFN-CERT-2011-0844, DFN-CERT-2011-0818, DFN-CERT-2011-0808, DFN-CERT-2011-0771, DFN-CERT-2011-0741, DFN-CERT-2011-0712, DFN-CERT-2011-0673, DFN-CERT-2011-0597, DFN-CERT-2011-0596, DFN-CERT-2011-0519, DFN-CERT-2011-0516, DFN-CERT-2011-0483, DFN-CERT-2011-0434, DFN-CERT-2011-0393, DFN-CERT-2011-0381

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

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

http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424

http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7

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

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

http://www.postfix.org/CVE-2011-0411.html
http://www.pureftpd.org/project/pure-ftpd/news
http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf
http://www.spamdyke.org/documentation/Changelog.txt
http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include_text=1
http://www.securityfocus.com/archive/1/516901
http://support.avaya.com/css/P8/documents/100134676
http://support.avaya.com/css/P8/documents/100141041
http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html
http://inoa.net/qmail-tls/vu555316.patch
http://www.kb.cert.org/vuls/id/555316

**Medium** (CVSS: 6.8) 5432/tcp
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105042)

**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.

**Affected Software/OS**

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

**Vulnerability Insight**

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

**Vulnerability Detection Method**

Send two SSL ChangeCipherSpec request and check the response.

Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105042)

Version used: $Revision: 12865 $

**References**

CVE: CVE-2014-0224
BID: 67899

CERT: CB-K15/0567, CB-K15/0415, CB-K15/0384, CB-K15/0080, CB-K15/0079, CB-K15/0074, CB-K14/1617, CB-K14/1537, CB-K14/1299, CB-K14/1297, CB-K14/1294, CB-K14/1202, CB-K14/1174, CB-K14/1153, CB-K14/0876, CB-K14/0756, CB-K14/0746, CB-K14/0736, CB-K14/0722, CB-K14/0716, CB-K14/0708, CB-K14/0684, CB-K14/0683, CB-K14/0680, DFN-CERT-2016-0388, DFN-CERT-2015-0593, DFN-CERT-2015-0427, DFN-CERT-2015-0396, DFN-CERT-2015-0082, DFN-CERT-2015-0079, DFN-CERT-2015-0078, DFN-CERT-2014-1717, DFN-CERT-2014-1632, DFN-CERT-2014-1364, DFN-CERT-2014-1357, DFN-CERT-2014-1350, DFN-CERT-2014-1265, DFN-CERT-2014-1209, DFN-CERT-2014-0917, DFN-CERT-2014-0789, DFN-CERT-2014-0778, DFN-CERT-2014-0768, DFN-CERT-2014-0752, DFN-CERT-2014-0747, DFN-CERT-2014-0738, DFN-CERT-2014-0715, DFN-CERT-2014-0714, DFN-CERT-2014-0709

Other: https://www.openssl.org/news/secadv/20140605.txt

http://www.securityfocus.com/bid/67899

http://openssl.org/

**Medium** (CVSS: 6.5) 80/tcp

NVT: Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.141885)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

**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.

**Affected 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: https://blog.ripstech.com/2018/scan-verify-patch-security-issues-in-minutes/

**Medium** (CVSS: 6.0) 80/tcp

NVT: TWiki Cross-Site Request Forgery Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.800400)

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

**Summary**

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

**Vulnerability Detection Result**

```
Installed version: 01.Feb.2003
Fixed version:     4.3.1
```

**Impact**

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

**Solution**

**Solution type:** VendorFix

Upgrade to version 4.3.1 or later.

**Affected Software/OS**

TWiki version prior to 4.3.1

**Vulnerability Insight**

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

**Vulnerability Detection Method**

Details: TWiki Cross-Site Request Forgery Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.800400)

Version used: $Revision: 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: http://secunia.com/advisories/34880
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258
http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff-cve-2009-1339.txt

**Medium** (CVSS: 5.8) 80/tcp

NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled (OID: 1.3.6.1.4.1.25623.1.0.11213)

**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.

**Vulnerability Detection Result**

```
The web server has the following HTTP methods enabled: TRACE
```

**Impact**

An attacker may use this flaw 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 configuration.

Please see the manual of your web server or the references for more information.

**Affected 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 |
| CERT: | CB-K14/0981, DFN-CERT-2014-1018, DFN-CERT-2010-0020 |
| Other: | http://www.kb.cert.org/vuls/id/288308 |
| | http://www.kb.cert.org/vuls/id/867593 |
| | http://httpd.apache.org/docs/current/de/mod/core.html#traceenable |
| | https://www.owasp.org/index.php/Cross_Site_Tracing |

**Medium** (CVSS: 5.0) 25/tcp
NVT: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

**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=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-
base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no
such thing outside US,C=XX
subject alternative names (SAN):
None
issued by .:
1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-
base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no
such thing outside 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): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436DE813CC
```

**Solution**

**Solution type:** Mitigation

Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**

Details: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Version used: $Revision: 11103 $

**Medium** (CVSS: 5.0) 5432/tcp
NVT: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

**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=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-
base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no
such thing outside US,C=XX
subject alternative names (SAN):
None
issued by .:
1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-
base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no
such thing outside 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): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436DE813CC
```

**Solution**

**Solution type:** Mitigation

Replace the SSL/TLS certificate by a new one.

**Vulnerability Insight**

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

**Vulnerability Detection Method**

Details: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Version used: $Revision: 11103 $

**Medium** (CVSS: 5.0) 80/tcp
NVT: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.800315)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

**Summary**

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

**Vulnerability Detection Result**

```
Installed version: 1.9.5
Fixed version:     2.2
```

**Impact**

Successful exploitation could allow arbitrary code execution in the context of an affected site.

**Solution**

**Solution type:** VendorFix

Upgrade to version 2.2 or later.

**Affected Software/OS**

Tiki Wiki CMS Groupware version prior to 2.2 on all running platform

**Vulnerability Insight**

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

**Vulnerability Detection Method**

Details: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.800315)

Version used: $Revision: 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: http://secunia.com/advisories/32341
http://info.tikiwiki.org/tiki-read_article.php?articleId=41

**Medium** (CVSS: 5.0) 80/tcp
NVT: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.108064)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

**Summary**

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

**Vulnerability Detection Result**

```
Installed version: 1.9.5
Fixed version:     12.11
```

**Impact**

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

**Solution**

**Solution type:** VendorFix

Upgrade to Tiki Wiki CMS Groupware version 12.11 LTS, 15.4 or later.

**Affected Software/OS**

Tiki Wiki CMS Groupware versions:

- below 12.11 LTS

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

**Vulnerability Insight**

The Flaw is due to improper sanitization of input passed to the 'fixedURLData' 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: http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-released
https://sourceforge.net/p/tikiwiki/code/60308/
https://tiki.org

**Medium** (CVSS: 5.0) 25/tcp
NVT: Check if Mailserver answer to VRFY and EXPN requests (OID: 1.3.6.1.4.1.25623.1.0.100072)

**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 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.

**Vulnerability Insight**

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.

**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: http://cr.yp.to/smtp/vrfy.html

**Medium** (CVSS: 4.8) 23/tcp
NVT: Telnet Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108522)

**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 sniffing traffic 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 $

**Medium** (CVSS: 4.8) 80/tcp
NVT: Cleartext Transmission of Sensitive Information via HTTP (OID: 1.3.6.1.4.1.25623.1.0.108440)

**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://192.168.1.98/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.

**Affected Software/OS**

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

**Vulnerability Detection Method**

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: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management
https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
https://cwe.mitre.org/data/definitions/319.html

**Medium** (CVSS: 4.3) 25/tcp

NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) (OID: 1.3.6.1.4.1.25623.1.0.805188)

**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 significantly 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.

**Affected 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 Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.

**Vulnerability Detection Method**

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 $

**References**

| | |
|---|---|
| CVE: | CVE-2015-4000 |
| BID: | 74733 |
| CERT: | CB-K16/1593, CB-K16/1552, CB-K16/0617, CB-K16/0599, CB-K16/0168, CB-K16/0121, CB-K16/0090, CB-K16/0030, CB-K15/1591, CB-K15/1550, CB-K15/1517, CB-K15/1464, CB-K15/1442, CB-K15/1334, CB-K15/1269, CB-K15/1136, CB-K15/1090, CB-K15/1059, CB-K15/1022, CB-K15/1015, CB-K15/0964, CB-K15/0932, CB-K15/0927, CB-K15/0926, CB-K15/0907, CB-K15/0901, CB-K15/0896, CB-K15/0877, CB-K15/0834, CB-K15/0802, CB-K15/0733, DFN-CERT-2016-1692, DFN-CERT-2016-1648, DFN-CERT-2016-0665, DFN-CERT-2016-0642, DFN-CERT-2016-0184, DFN-CERT-2016-0135, DFN-CERT-2016-0101, DFN-CERT-2016-0035, DFN-CERT-2015-1679, DFN-CERT-2015-1632, DFN-CERT-2015-1608, DFN-CERT-2015-1542, DFN-CERT-2015-1518, DFN-CERT-2015-1406, DFN-CERT-2015-1341, DFN-CERT-2015-1194, DFN-CERT-2015-1144, DFN-CERT-2015-1113, DFN-CERT-2015-1078, DFN-CERT-2015-1067, DFN-CERT-2015-1016, DFN-CERT-2015-0980, DFN-CERT-2015-0977, DFN-CERT-2015-0976, DFN-CERT-2015-0960, DFN-CERT-2015-0956, DFN-CERT-2015-0944, DFN-CERT-2015-0925, DFN-CERT-2015-0879, DFN-CERT-2015-0844, DFN-CERT-2015-0737 |
| Other: | https://weakdh.org<br>https://weakdh.org/imperfect-forward-secrecy.pdf<br>http://openwall.com/lists/oss-security/2015/05/20/8<br>https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained<br>https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes |

**Medium** (CVSS: 4.3) 5432/tcp

NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

**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 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT.

**Impact**

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

**Solution**

**Solution type:** Mitigation

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

**Affected Software/OS**

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**

The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:

- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)

- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

**Vulnerability Detection Method**

Check the used protocols of the services provided by this system.

Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

Version used: $Revision: 5547 $

**References**

CVE: CVE-2016-0800, CVE-2014-3566

CERT: CB-K18/0094, CB-K17/1198, CB-K17/1196, CB-K16/1828, CB-K16/1438, CB-K16/1384, CB-K16/1141, CB-K16/1107, CB-K16/1102, CB-K16/0792, CB-K16/0599, CB-K16/0597, CB-K16/0459, CB-K16/0456, CB-K16/0433, CB-K16/0424, CB-K16/0415, CB-K16/0413, CB-K16/0374, CB-K16/0367, CB-K16/0331, CB-K16/0329, CB-K16/0328, CB-K16/0156, CB-K15/1514, CB-K15/1358, CB-K15/1021, CB-K15/0972, CB-K15/0637, CB-K15/0590, CB-K15/0525, CB-K15/0393, CB-K15/0384, CB-K15/0287, CB-K15/0252, CB-K15/0246, CB-K15/0237, CB-K15/0118, CB-K15/0110, CB-K15/0108, CB-K15/0080, CB-K15/0078, CB-K15/0077, CB-K15/0075, CB-K14/1617, CB-K14/1581, CB-K14/1537, CB-K14/1479, CB-K14/1458, CB-K14/1342, CB-K14/1314, CB-K14/1313, CB-K14/1311, CB-K14/1304, CB-K14/1296, DFN-CERT-2018-0096, DFN-CERT-2017-1238, DFN-CERT-2017-1236, DFN-CERT-2016-1929, DFN-CERT-2016-1527, DFN-CERT-2016-1468, DFN-CERT-2016-1216, DFN-CERT-2016-1174, DFN-CERT-2016-1168, DFN-CERT-2016-0884, DFN-CERT-2016-0841, DFN-CERT-2016-0644, DFN-CERT-2016-0642, DFN-CERT-2016-0496, DFN-CERT-2016-0495, DFN-CERT-2016-0465, DFN-CERT-2016-0459, DFN-CERT-2016-0453, DFN-CERT-2016-0451, DFN-CERT-2016-0415, DFN-CERT-2016-0403, DFN-CERT-2016-0388, DFN-CERT-2016-0360, DFN-CERT-2016-0359, DFN-CERT-2016-0357, DFN-CERT-2016-0171, DFN-CERT-2015-1431, DFN-CERT-2015-1075, DFN-CERT-2015-1026, DFN-CERT-2015-0664, DFN-CERT-2015-0548, DFN-CERT-2015-0404, DFN-CERT-2015-0396, DFN-CERT-2015-0259, DFN-CERT-2015-0254, DFN-CERT-2015-0245, DFN-CERT-2015-0118, DFN-CERT-2015-0114, DFN-CERT-2015-0083, DFN-CERT-2015-0082, DFN-CERT-2015-0081, DFN-CERT-2015-0076, DFN-CERT-2014-1717, DFN-CERT-2014-1680, DFN-CERT-2014-1632, DFN-CERT-2014-1564, DFN-CERT-2014-1542, DFN-CERT-2014-1414, DFN-CERT-2014-1366, DFN-CERT-2014-1354

Other: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

https://bettercrypto.org/

https://mozilla.github.io/server-side-tls/ssl-config-generator/

https://drownattack.com/

https://www.imperialviolet.org/2014/10/14/poodle.html

**Medium** (CVSS: 4.3) 25/tcp

NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

**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 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.
```

**Impact**

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

**Solution**

**Solution type:** Mitigation

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

**Affected Software/OS**

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**

The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:

- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)

- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

**Vulnerability Detection Method**

Check the used protocols of the services provided by this system.

Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

Version used: $Revision: 5547 $

**References**

CVE: CVE-2016-0800, CVE-2014-3566

CERT: CB-K18/0094, CB-K17/1198, CB-K17/1196, CB-K16/1828, CB-K16/1438, CB-K16/1384, CB-K16/1141, CB-K16/1107, CB-K16/1102, CB-K16/0792, CB-K16/0599, CB-K16/0597, CB-K16/0459, CB-K16/0456, CB-K16/0433, CB-K16/0424, CB-K16/0415, CB-K16/0413, CB-K16/0374, CB-K16/0367, CB-K16/0331, CB-K16/0329, CB-K16/0328, CB-K16/0156, CB-K15/1514, CB-K15/1358, CB-K15/1021, CB-K15/0972, CB-K15/0637, CB-K15/0590, CB-K15/0525, CB-K15/0393, CB-K15/0384, CB-K15/0287, CB-K15/0252, CB-K15/0246, CB-K15/0237, CB-K15/0118, CB-K15/0110, CB-K15/0108, CB-K15/0080, CB-K15/0078, CB-K15/0077, CB-K15/0075, CB-K14/1617, CB-K14/1581, CB-K14/1537, CB-K14/1479, CB-K14/1458, CB-K14/1342, CB-K14/1314, CB-K14/1313, CB-K14/1311, CB-K14/1304, CB-K14/1296, DFN-CERT-2018-0096, DFN-CERT-2017-1238, DFN-CERT-2017-1236, DFN-CERT-2016-1929, DFN-CERT-2016-1527, DFN-CERT-2016-1468, DFN-CERT-2016-1216, DFN-CERT-2016-1174, DFN-CERT-2016-1168, DFN-CERT-2016-0884, DFN-CERT-2016-0841, DFN-CERT-2016-0644, DFN-CERT-2016-0642, DFN-CERT-2016-0496, DFN-CERT-2016-0495, DFN-CERT-2016-0465, DFN-CERT-2016-0459, DFN-CERT-2016-0453, DFN-CERT-2016-0451, DFN-CERT-2016-0415, DFN-CERT-2016-0403, DFN-CERT-2016-0388, DFN-CERT-2016-0360, DFN-CERT-2016-0359, DFN-CERT-2016-0357, DFN-CERT-2016-0171, DFN-CERT-2015-1431, DFN-CERT-2015-1075,

DFN-CERT-2015-1026, DFN-CERT-2015-0664, DFN-CERT-2015-0548, DFN-CERT-2015-0404, DFN-CERT-2015-0396, DFN-CERT-2015-0259, DFN-CERT-2015-0254, DFN-CERT-2015-0245, DFN-CERT-2015-0118, DFN-CERT-2015-0114, DFN-CERT-2015-0083, DFN-CERT-2015-0082, DFN-CERT-2015-0081, DFN-CERT-2015-0076, DFN-CERT-2014-1717, DFN-CERT-2014-1680, DFN-CERT-2014-1632, DFN-CERT-2014-1564, DFN-CERT-2014-1542, DFN-CERT-2014-1414, DFN-CERT-2014-1366, DFN-CERT-2014-1354

Other: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

https://bettercrypto.org/

https://mozilla.github.io/server-side-tls/ssl-config-generator/

https://drownattack.com/

https://www.imperialviolet.org/2014/10/14/poodle.html

**Medium** (CVSS: 4.3) 80/tcp

NVT: Apache Web Server ETag Header Information Disclosure Weakness (OID: 1.3.6.1.4.1.25623.1.0.103122)

**Summary**

A weakness has been discovered in Apache web servers that are configured to use the FileETag directive.

**Vulnerability Detection Result**

```
Information that was gathered:
Inode: 67575
Size: 45
```

**Impact**

Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.

**Solution**

**Solution type:** VendorFix

OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.

Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

**Vulnerability Detection Method**

Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.

Details: Apache Web Server ETag Header Information Disclosure Weakness (OID: 1.3.6.1.4.1.25623.1.0.103122)

Version used: $Revision: 11997 $

**References**

CVE: CVE-2003-1418

BID: 6939

CERT: CB-K17/1750, CB-K17/0896, CB-K15/0469, DFN-CERT-2017-1821, DFN-CERT-2017-0925, DFN-CERT-2015-0495

Other: https://www.securityfocus.com/bid/6939

http://httpd.apache.org/docs/mod/core.html#fileetag

http://www.openbsd.org/errata32.html

http://support.novell.com/docs/Tids/Solutions/10090670.html

**Medium** (CVSS: 4.3) 25/tcp
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) (OID: 1.3.6.1.4.1.25623.1.0.805142)

**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 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.

**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.

**Affected 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**

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

CERT: CB-K18/0799, CB-K16/1289, CB-K16/1096, CB-K15/1751, CB-K15/1266, CB-K15/0850, CB-K15/0764, CB-K15/0720, CB-K15/0548, CB-K15/0526, CB-K15/0509, CB-K15/0493, CB-K15/0384, CB-K15/0365, CB-K15/0364, CB-K15/0302, CB-K15/0192, CB-K15/0016, DFN-CERT-2018-1408, DFN-CERT-2016-1372, DFN-

CERT-2016-1164, DFN-CERT-2016-0388, DFN-CERT-2015-1853, DFN-CERT-2015-1332, DFN-CERT-2015-0884, DFN-CERT-2015-0800, DFN-CERT-2015-0758, DFN-CERT-2015-0567, DFN-CERT-2015-0544, DFN-CERT-2015-0530, DFN-CERT-2015-0396, DFN-CERT-2015-0375, DFN-CERT-2015-0374, DFN-CERT-2015-0305, DFN-CERT-2015-0199, DFN-CERT-2015-0021

Other: https://freakattack.com

http://secpod.org/blog/?p=3818

http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html

https://www.openssl.org

**Medium** (CVSS: 4.3) 5432/tcp

NVT: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)

**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 configured 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 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.

**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 $

**References**

CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000

CERT: CB-K17/1750, CB-K16/1593, CB-K16/1552, CB-K16/1102, CB-K16/0617, CB-K16/0599, CB-K16/0168, CB-K16/0121, CB-K16/0090, CB-K16/0030, CB-K15/1751, CB-K15/1591, CB-K15/1550, CB-K15/1517, CB-K15/1514, CB-K15/1464, CB-K15/1442, CB-K15/1334, CB-K15/1269, CB-K15/1136, CB-K15/1090, CB-K15/1059, CB-K15/1022, CB-K15/1015, CB-K15/0986, CB-K15/0964, CB-K15/0962, CB-K15/0932, CB-K15/0927, CB-K15/0926, CB-K15/0907, CB-K15/0901, CB-K15/0896, CB-K15/0889, CB-K15/0877, CB-K15/0850, CB-K15/0849, CB-K15/0834, CB-K15/0827, CB-K15/0802, CB-K15/0764, CB-K15/0733, CB-K15/0667, CB-K14/0935, CB-K13/0942, DFN-CERT-2017-1821, DFN-CERT-2016-1692, DFN-CERT-2016-1648, DFN-CERT-2016-1168, DFN-CERT-2016-0665, DFN-CERT-2016-0642, DFN-CERT-2016-0184, DFN-CERT-2016-0135, DFN-CERT-2016-0101, DFN-CERT-2016-0035, DFN-CERT-2015-1853, DFN-CERT-2015-1679, DFN-CERT-2015-1632, DFN-CERT-2015-1608, DFN-CERT-2015-1542, DFN-CERT-2015-1518, DFN-CERT-2015-1406, DFN-CERT-2015-1341, DFN-CERT-2015-1194, DFN-CERT-2015-1144, DFN-CERT-2015-1113, DFN-CERT-2015-1078, DFN-CERT-2015-1067, DFN-CERT-2015-1038, DFN-CERT-2015-1016, DFN-CERT-2015-1012, DFN-CERT-2015-0980, DFN-CERT-2015-0977, DFN-CERT-2015-0976, DFN-CERT-2015-0960, DFN-CERT-2015-0956, DFN-CERT-2015-0944, DFN-CERT-2015-0937, DFN-CERT-2015-0925, DFN-CERT-2015-0884, DFN-CERT-2015-0881, DFN-CERT-2015-0879, DFN-CERT-2015-0866, DFN-CERT-2015-0844, DFN-CERT-2015-0800, DFN-CERT-2015-0737, DFN-CERT-2015-0696, DFN-CERT-2014-0977

Other: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html

https://bettercrypto.org/

https://mozilla.github.io/server-side-tls/ssl-config-generator/

---

**Medium** (CVSS: 4.3) 5432/tcp

NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ... (OID: 1.3.6.1.4.1.25623.1.0.802087)

**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)

Version used: $Revision: 11402 $

**References**

CVE: CVE-2014-3566

BID: 70574

CERT: CB-K17/1198, CB-K17/1196, CB-K16/1828, CB-K16/1438, CB-K16/1384, CB-K16/1102, CB-K16/0599, CB-K16/0156, CB-K15/1514, CB-K15/1358, CB-K15/1021, CB-K15/0972, CB-K15/0637, CB-K15/0590, CB-K15/0525, CB-K15/0393, CB-K15/0384, CB-K15/0287, CB-K15/0252, CB-K15/0246, CB-K15/0237, CB-K15/0118, CB-K15/0110, CB-K15/0108, CB-K15/0080, CB-K15/0078, CB-K15/0077, CB-K15/0075, CB-K14/1617, CB-K14/1581, CB-K14/1537, CB-K14/1479, CB-K14/1458, CB-K14/1342, CB-K14/1314, CB-K14/1313, CB-K14/1311, CB-K14/1304, CB-K14/1296, DFN-CERT-2017-1238, DFN-CERT-2017-1236, DFN-CERT-2016-1929, DFN-CERT-2016-1527, DFN-CERT-2016-1468, DFN-CERT-2016-1168, DFN-CERT-2016-0884, DFN-CERT-2016-0642, DFN-CERT-2016-0388, DFN-CERT-2016-0171, DFN-CERT-2015-1431, DFN-CERT-2015-1075, DFN-CERT-2015-1026, DFN-CERT-2015-0664, DFN-CERT-2015-0548, DFN-CERT-2015-0404, DFN-CERT-2015-0396, DFN-CERT-2015-0259, DFN-CERT-2015-0254, DFN-CERT-2015-0245, DFN-CERT-2015-0118, DFN-CERT-2015-0114, DFN-CERT-2015-0083, DFN-CERT-2015-0082, DFN-CERT-2015-0081, DFN-CERT-2015-0076, DFN-CERT-2014-1717, DFN-CERT-2014-1680, DFN-CERT-2014-1632, DFN-CERT-2014-1564, DFN-CERT-2014-1542, DFN-CERT-2014-1414, DFN-CERT-2014-1366, DFN-CERT-2014-1354

Other: https://www.openssl.org/~bodo/ssl-poodle.pdf

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html

http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

**Medium** (CVSS: 4.3) 25/tcp

NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ... (OID: 1.3.6.1.4.1.25623.1.0.802087)

**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)

Version used: $Revision: 11402 $

**References**

CVE: CVE-2014-3566

BID: 70574

CERT: CB-K17/1198, CB-K17/1196, CB-K16/1828, CB-K16/1438, CB-K16/1384, CB-K16/1102, CB-K16/0599, CB-K16/0156, CB-K15/1514, CB-K15/1358, CB-K15/1021, CB-K15/0972, CB-K15/0637, CB-K15/0590, CB-K15/0525, CB-K15/0393, CB-K15/0384, CB-K15/0287, CB-K15/0252, CB-K15/0246, CB-K15/0237, CB-K15/0118, CB-K15/0110, CB-K15/0108, CB-K15/0080, CB-K15/0078, CB-K15/0077, CB-K15/0075, CB-K14/1617, CB-K14/1581, CB-K14/1537, CB-K14/1479, CB-K14/1458, CB-K14/1342, CB-K14/1314, CB-K14/1313, CB-K14/1311, CB-K14/1304, CB-K14/1296, DFN-CERT-2017-1238, DFN-CERT-2017-1236, DFN-CERT-2016-1929, DFN-CERT-2016-1527, DFN-CERT-2016-1468, DFN-CERT-2016-1168, DFN-CERT-2016-0884, DFN-CERT-2016-0642, DFN-CERT-2016-0388, DFN-CERT-2016-0171, DFN-CERT-2015-1431, DFN-CERT-2015-1075, DFN-CERT-2015-1026, DFN-CERT-2015-0664, DFN-CERT-2015-0548, DFN-CERT-2015-0404, DFN-CERT-2015-0396, DFN-CERT-2015-0259, DFN-CERT-2015-0254, DFN-CERT-2015-0245, DFN-CERT-2015-0118, DFN-CERT-2015-0114, DFN-CERT-2015-0083, DFN-CERT-2015-0082, DFN-CERT-2015-0081, DFN-CERT-2015-0076, DFN-CERT-2014-1717, DFN-CERT-2014-1680, DFN-CERT-2014-1632, DFN-CERT-2014-1564, DFN-CERT-2014-1542, DFN-CERT-2014-1414, DFN-CERT-2014-1366, DFN-CERT-2014-1354

Other: https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

---

**Medium** (CVSS: 4.3) 80/tcp

NVT: TWiki < 6.1.0 XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.141830)

Product detection result: cpe:/a:twiki:twiki:01.Feb.2003 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.

**Affected 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

Method: TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

**References**

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

**Medium** (CVSS: 4.3) 22/tcp
NVT: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611)

**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.

The `none` algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**

Check if remote ssh service supports Arcfour, none or CBC ciphers.

Details: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611)

Version used: $Revision: 13581 $

**References**

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

**Medium** (CVSS: 4.3) 80/tcp
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902830)

**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.

**Affected Software/OS**

Apache HTTP Server versions 2.2.0 through 2.2.21

**Vulnerability Insight**

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

**Vulnerability Detection Method**

Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902830)

Version used: $Revision: 11857 $

**References**

CVE: CVE-2012-0053

BID: 51706

CERT: CB-K15/0080, CB-K14/1505, CB-K14/0608, DFN-CERT-2015-0082, DFN-CERT-2014-1592, DFN-CERT-2014-0635, DFN-CERT-2013-1307, DFN-CERT-2012-1276, DFN-CERT-2012-1112, DFN-CERT-2012-0928, DFN-CERT-2012-0758, DFN-CERT-2012-0744, DFN-CERT-2012-0568, DFN-CERT-2012-0425, DFN-CERT-2012-0424, DFN-CERT-2012-0387, DFN-CERT-2012-0343, DFN-CERT-2012-0332, DFN-CERT-2012-0306, DFN-CERT-2012-0264, DFN-CERT-2012-0203, DFN-CERT-2012-0188

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

**Medium** (CVSS: 4.3) 80/tcp
NVT: Tiki Wiki CMS Groupware Multiple Cross Site Scripting Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.800266)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

**Summary**

This host is running Tiki Wiki CMS Groupware and is prone to Multiple Cross Site Scripting vulnerabilities.

**Vulnerability Detection Result**

```
Vulnerable url: http://192.168.1.98/tikiwiki/tiki-listpages.php/<script>alert("XSS_Check");</script>
```

**Impact**

Successful exploitation will allow remote attackers to inject arbitrary HTML codes in the context of the affected web application.

**Solution**

**Solution type:** VendorFix

Upgrade to Tiki Wiki CMS Groupware version 2.4 or later.

**Affected Software/OS**

Tiki Wiki CMS Groupware version 2.2, 2.3 and prior.

**Vulnerability Insight**

Multiple flaws are due to improper sanitization of user supplied input in the pages i.e. 'tiki-orphan_pages.php', 'tiki-listpages.php', 'tiki-list_file_gallery.php' and 'tiki-galleries.php' which lets the attacker conduct XSS attacks inside the context of the web application.

**Vulnerability Detection Method**

Details: Tiki Wiki CMS Groupware Multiple Cross Site Scripting Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.800266)

Version used: $Revision: 14031 $

**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-2009-1204 |
| BID: | 34105, 34106, 34107, 34108 |
| Other: | http://secunia.com/advisories/34273 |
| | http://info.tikiwiki.org/tiki-read_article.php?articleId=51 |

**Medium** (CVSS: 4.0) 5432/tcp

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

**Summary**

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

**Vulnerability Detection Result**

```
Server Temporary Key Size: 1024 bits
```

**Impact**

An attacker might be able to decrypt the SSL/TLS communication offline.

**Solution**

**Solution type:** Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see 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 Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

**Vulnerability Detection Method**

Checks the DHE temporary public key size.

Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: $Revision: 12865 $

**References**

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

**Medium** (CVSS: 4.0) 25/tcp
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

**Summary**

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

**Vulnerability Detection Result**

```
Server Temporary Key Size: 1024 bits
```

**Impact**

An attacker might be able to decrypt the SSL/TLS communication offline.

**Solution**

**Solution type:** Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see 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 Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and

768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

**Vulnerability Detection Method**

Checks the DHE temporary public key size.

Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: $Revision: 12865 $

**References**

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

**Medium** (CVSS: 4.0) 5432/tcp
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

**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=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-
base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no
such thing 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**

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 $

**References**

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

**Low** (CVSS: 3.5) 80/tcp

NVT: Tiki Wiki CMS Groupware XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.140797)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 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/filegals/filegallib.php.

**Vulnerability Detection Result**

```
Installed version: 1.9.5
Fixed version:     18.0
```

**Solution**

**Solution type:** VendorFix

Upgrade to version 18.0 or later.

**Affected 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: http://openwall.com/lists/oss-security/2018/02/16/1

**Low** (CVSS: 2.6) 22/tcp

NVT: SSH Weak MAC Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105610)

**Summary**

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

**Vulnerability Detection Result**

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

hmac-md5
hmac-md5-96
hmac-sha1-96


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

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 $

This file was automatically generated.