Scan Report

November 13, 2020

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 "New Quick Task". The scan started at Fri Nov 13 04:25:46 2020 UTC and ended at Fri Nov 13 04:46:32 2020 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.2.4 owasp	20	76	9	0	0
Total: 1	20	76	9	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
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.
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 105 results selected by the filtering described above. Before filtering there were 709 results.

1.1 Host Authentications

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

2 Results per Host

2.1 10.0.2.4

Host scan start Fri Nov 13 04:26:01 2020 UTC
Host scan end Fri Nov 13 04:44:41 2020 UTC

Service (Port)	Threat Level
8080/tcp	High
80/tcp	High
general/tcp	High
443/tcp	High
8080/tcp	Medium
80/tcp	Medium
8081/tcp	Medium
22/tcp	Medium
443/tcp	Medium

. . . (continues) . . .

. . . (continued) . . .

Service (Port)	Threat Level
80/tcp	Low
general/tcp	Low
22/tcp	Low
443/tcp	Low

2.1.1 High 8080/tcp

High (CVSS: 10.0)
NVT: Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials

Product detection result

```
cpe:/a:apache:tomcat:6.0.24
Detected by Apache Tomcat Detection (Consolidation) (OID: 1.3.6.1.4.1.25623.1.0.
↪107652)
```

Summary

The Apache Tomcat Manager/Host Manager/Server Status is using default or known hardcoded credentials.

Vulnerability Detection Result

```
It was possible to login into the Tomcat Host Manager at http://owasp:8080/host-
↪manager/html using user "root" with password "owaspbwa"
It was possible to login into the Tomcat Manager at http://owasp:8080/manager/ht
↪ml using user "root" with password "owaspbwa"
It was possible to login into the Tomcat Server Status at http://owasp:8080/mana
↪ger/status using user "root" with password "owaspbwa"
```

Impact

An attacker can exploit this issue to upload and execute arbitrary code, which will facilitate a complete compromise of the affected computer.

Solution

Solution type: Mitigation

Change the password to a strong one or remove the user from tomcat-users.xml.

Vulnerability Detection Method

Details: `Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials`

OID:1.3.6.1.4.1.25623.1.0.103550

Product Detection Result

Product: `cpe:/a:apache:tomcat:6.0.24`

Method: `Apache Tomcat Detection (Consolidation)`

OID: 1.3.6.1.4.1.25623.1.0.107652)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2010-4094
cve: CVE-2009-3548
cve: CVE-2009-4189
cve: CVE-2009-3099
cve: CVE-2009-3843
cve: CVE-2009-4188
cve: CVE-2010-0557
bid: 44172
bid: 36954
bid: 79264
bid: 79351
bid: 37086
bid: 36258
bid: 38084
url: https://www.zerodayinitiative.com/advisories/ZDI-10-214/
url: https://www.zerodayinitiative.com/advisories/ZDI-09-085/
dfn-cert: DFN-CERT-2012-1832
dfn-cert: DFN-CERT-2011-0185
dfn-cert: DFN-CERT-2010-0801
dfn-cert: DFN-CERT-2010-0690
dfn-cert: DFN-CERT-2009-1640
```

[return to 10.0.2.4]

2.1.2 High 80/tcp

High (CVSS: 10.0)
NVT: Tiki Wiki CMS Groupware End of Life Detection

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 Tiki Wiki CMS Groupware version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

```
The "Tiki Wiki CMS Groupware" version on the remote host has reached the end of
↪life.
CPE:               cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Installed version: 1.9.5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Location/URL:       /tikiwiki
EOL version:        1
EOL date:           unknown
EOL info:           https://tiki.org/Versions#Version_Lifecycle
```

Impact

An end of life version of Tiki Wiki CMS Groupware is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

Solution type: VendorFix

Update the Tiki Wiki CMS Groupware version on the remote host to a still supported version.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Tiki Wiki CMS Groupware End of Life Detection`

OID:1.3.6.1.4.1.25623.1.0.108622

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

url: `https://tiki.org/Versions#Version_Lifecycle`

High (CVSS: 7.8)

NVT: Apache httpd Web Server Range Header Denial of Service Vulnerability

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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

References

```
cve: CVE-2011-3192
bid: 49303
url: http://www.exploit-db.com/exploits/17696
url: http://packetstormsecurity.org/files/view/104441
url: http://marc.info/?l=apache-httpd-dev&m=131420013520206&w=2
url: http://mail-archives.apache.org/mod_mbox/httpd-dev/201108.mbox/%3CCAAPSnn2P
↪O-d-C4nQt_TES2RRWiZr7urefhTKPWBC1b+K1Dqc7g@mail.gmail.com%3E
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-0856
dfn-cert: DFN-CERT-2012-0746
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2011-1726
dfn-cert: DFN-CERT-2011-1725
dfn-cert: DFN-CERT-2011-1693
dfn-cert: DFN-CERT-2011-1692
dfn-cert: DFN-CERT-2011-1632
dfn-cert: DFN-CERT-2011-1631
dfn-cert: DFN-CERT-2011-1593
dfn-cert: DFN-CERT-2011-1519
dfn-cert: DFN-CERT-2011-1492
dfn-cert: DFN-CERT-2011-1440
dfn-cert: DFN-CERT-2011-1435
dfn-cert: DFN-CERT-2011-1430
dfn-cert: DFN-CERT-2011-1429
dfn-cert: DFN-CERT-2011-1425
dfn-cert: DFN-CERT-2011-1379
dfn-cert: DFN-CERT-2011-1362
dfn-cert: DFN-CERT-2011-1343
dfn-cert: DFN-CERT-2011-1342
dfn-cert: DFN-CERT-2011-1341
dfn-cert: DFN-CERT-2011-1335
dfn-cert: DFN-CERT-2011-1333
dfn-cert: DFN-CERT-2011-1318
dfn-cert: DFN-CERT-2011-1312
dfn-cert: DFN-CERT-2011-1298
```

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

Product detection result

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

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

Vulnerability Detection Result

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

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

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

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

Vulnerability Detection Method
Details: `Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100537

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: CVE-2010-1134
cve: CVE-2010-1133
cve: CVE-2010-1136
bid: 38608
url: http://www.securityfocus.com/bid/38608
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=24734
url: http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25046
url: http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25424
url: http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25435
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: Joomla < 3.9.5 Multiple Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

Joomla! is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.9.5
Installation
path / port:       /joomla
```

Impact

Successful exploitation would allow an attacker to access sensitive information or execute arbitrary commands.

Solution

Solution type: VendorFix

Update to version 3.9.5.

Affected Software/OS

Joomla! through version 3.9.4.

Vulnerability Insight

The following vulnerabilities exist:

- The Media Manager component does not properly sanitize the folder parameter, allowing attackers to act outside the media manager root directory
- The 'refresh list of helpsites' endpoint of com_users lacks access checks, allowing calls from unauthenticated users
- The $.extend method of JQuery is vulnerable to Object.prototype pollution attacks (CVE-2019-11358)

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Joomla < 3.9.5 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.113369

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2019-10945
cve: CVE-2019-10946
cve: CVE-2019-11358
url: https://developer.joomla.org/security-centre/777-20190401-core-directory-tr
↪aversal-in-com-media
url: https://developer.joomla.org/security-centre/778-20190402-core-helpsites-re
↪fresh-endpoint-callable-for-unauthenticated-users
url: https://developer.joomla.org/security-centre.html
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K20/0800
cert-bund: CB-K20/0710
cert-bund: CB-K20/0324
cert-bund: CB-K20/0314
cert-bund: CB-K20/0309
cert-bund: CB-K20/0106
cert-bund: CB-K20/0041
cert-bund: CB-K20/0037
cert-bund: CB-K20/0034
cert-bund: CB-K19/0921
cert-bund: CB-K19/0920
cert-bund: CB-K19/0916
cert-bund: CB-K19/0911
cert-bund: CB-K19/0909
cert-bund: CB-K19/0619
cert-bund: CB-K19/0504
cert-bund: CB-K19/0287
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1574
dfn-cert: DFN-CERT-2020-1537
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0769
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0721
dfn-cert: DFN-CERT-2020-0276
dfn-cert: DFN-CERT-2020-0102
dfn-cert: DFN-CERT-2020-0100
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-2156
dfn-cert: DFN-CERT-2019-2126
dfn-cert: DFN-CERT-2019-1861
dfn-cert: DFN-CERT-2019-1663
dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1182
dfn-cert: DFN-CERT-2019-1153
dfn-cert: DFN-CERT-2019-1118
dfn-cert: DFN-CERT-2019-1033
dfn-cert: DFN-CERT-2019-0914
dfn-cert: DFN-CERT-2019-0899
dfn-cert: DFN-CERT-2019-0805
dfn-cert: DFN-CERT-2019-0723
```

High (CVSS: 7.5)
NVT: Joomla! Prior to 1.6.1 Multiple Security Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

Joomla! is prone to multiple security vulnerabilities including:
- An SQL-injection issue
- A path-disclosure vulnerability
- Multiple cross-site scripting issues
- Multiple information-disclosure vulnerabilities
- A URI-redirection vulnerability
- A security-bypass vulnerability
- A cross-site request-forgery vulnerability
- A denial-of-service vulnerability

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     1.6.1
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

An attacker can exploit these vulnerabilities to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, steal cookie-based authentication credentials, disclose or modify sensitive information, exploit latent vulnerabilities in the underlying database, deny service to legitimate users, redirect a victim to a potentially malicious site, or perform unauthorized actions. Other attacks are also possible.

Solution
Solution type: VendorFix
The vendor released a patch. Please see the references for more information.

Affected Software/OS
Versions prior to Joomla! 1.6.1 are vulnerable.

Vulnerability Detection Method
Details: `Joomla! Prior to 1.6.1 Multiple Security Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.103114

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
bid: 46787
url: https://www.securityfocus.com/bid/46787
url: http://www.joomla.org/announcements/release-news/5350-joomla-161-released.h
↪tml
```

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

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

Vulnerability Detection Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://owasp/bWAPP/phpinfo.php
http://owasp/mutillidae/phpinfo.php
http://owasp/vicnum/test.php
http://owasp/vicnum/test.php?mode=phpinfo
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

High (CVSS: 7.5)
NVT: Joomla! < 3.9.7 Multiple Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary
Joomla! is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.9.7
Installation
path / port:       /joomla
```

Impact
Successful exploitation can have effects ranging from disclosure of sensitive information to executing arbitrary code on the target machine.

Solution
Solution type: VendorFix
Update to version 3.9.7.

Affected Software/OS
Joomla! through version 3.9.6.

Vulnerability Insight
The following vulnerabilities exist:
- The update server URL of com_joomlaupdate can be manipulated by non Super-Admin users.
- The subform fieldtype does not sufficiently filter or validate input of subfields. This leads to XSS attack vectors.
- The CSV export of com_actionslogs is vulnerable to CSV injection.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Joomla! < 3.9.7 Multiple Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.113390

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`

Method: `joomla Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2019-12764
cve: CVE-2019-12765
cve: CVE-2019-12766
bid: 108729
bid: 108735
bid: 108736
url: https://developer.joomla.org/security-centre/785-20190603-core-acl-hardenin
↪g-of-com-joomlaupdate
url: https://developer.joomla.org/security-centre/783-20190601-core-csv-injectio
↪n-in-com-actionlogs
url: https://developer.joomla.org/security-centre/784-20190602-core-xss-in-subfo
↪rm-field
cert-bund: CB-K19/0495
dfn-cert: DFN-CERT-2019-1179
```

High (CVSS: 7.5)

NVT: WordPress Spreadsheet plugin Multiple Vulnerabilities

Product detection result

```
cpe:/a:wordpress:wordpress:2.0
Detected by WordPress Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900182)
```

Summary

This host is installed with WordPress Spreadsheet plugin and is prone to multiple vulnerabilities.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to execute arbitrary HTML and script code in a users browser session in the context of an affected site and inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.

. . . continues on next page . . .

. . . continued from previous page . . .

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.

Affected Software/OS
WordPress Spreadsheet plugin version 0.62

Vulnerability Insight
Input passed via the 'ss_id' parameter to wpSS/ss_handler.php script is not validated before returning it to users.

Vulnerability Detection Method
Send a crafted data via HTTP GET request and check whether it is able to read cookie or not.
Details: `WordPress Spreadsheet plugin Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.804872

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:2.0`
Method: `WordPress Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900182)

References
```
cve: CVE-2014-8363
cve: CVE-2014-8364
bid: 69073
bid: 69089
url: http://packetstormsecurity.com/files/127770
```

High (CVSS: 7.5)
NVT: Joomla! < 3.8.12 Multiple Vulnerabilities

Product detection result
```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary
This host is running Joomla and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.5.15
Fixed version:     3.8.12
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

`path / port:        /joomla`

Solution
Solution type: VendorFix
Upgrade to version 3.8.12 or later.

Affected Software/OS
Joomla! CMS versions 1.5.0 through 3.8.11

Vulnerability Insight
The following vulnerabilities exist:
- Inadequate output filtering on the user profile page could lead to a stored XSS attack. (CVE-2018-15880)
- Inadequate checks in the InputFilter class could allow specifically prepared PHAR files to pass the upload filter. (CVE-2018-15882)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! < 3.8.12 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.112371

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2018-15880
cve: CVE-2018-15882
url: https://developer.joomla.org/security-centre/744-20180802-core-stored-xss-v
↪ulnerability-in-the-frontend-profile.html
url: https://developer.joomla.org/security-centre/743-20180801-core-hardening-th
↪e-inputfilter-for-phar-stubs.html
dfn-cert: DFN-CERT-2018-1744
```

[return to 10.0.2.4]

2.1.3 High general/tcp

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

Product detection result

```
cpe:/o:canonical:ubuntu_linux:10.04
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪.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:10.04
Installed version,
build or SP:       10.04
EOL date:          2015-04-30
EOL info:          https://wiki.ubuntu.com/Releases
```

Solution
Solution type: Mitigation
Upgrade the Operating System on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method
Details: `OS End Of Life Detection`
OID:1.3.6.1.4.1.25623.1.0.103674

Product Detection Result
Product: `cpe:/o:canonical:ubuntu_linux:10.04`
Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 10.0.2.4]

2.1.4 High 443/tcp

High (CVSS: 10.0)
NVT: Tiki Wiki CMS Groupware End of Life Detection

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 Tiki Wiki CMS Groupware version on the remote host has reached the end of life and should not be used anymore.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The "Tiki Wiki CMS Groupware" version on the remote host has reached the end of
↪life.
CPE:               cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Installed version: 1.9.5
Location/URL:      /tikiwiki
EOL version:       1
EOL date:          unknown
EOL info:          https://tiki.org/Versions#Version_Lifecycle
```

Impact

An end of life version of Tiki Wiki CMS Groupware is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

Solution type: VendorFix

Update the Tiki Wiki CMS Groupware version on the remote host to a still supported version.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Tiki Wiki CMS Groupware End of Life Detection`

OID:1.3.6.1.4.1.25623.1.0.108622

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

url: `https://tiki.org/Versions#Version_Lifecycle`

High (CVSS: 7.8)

NVT: Apache httpd Web Server Range Header Denial of Service Vulnerability

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

References

```
cve: CVE-2011-3192
bid: 49303
url: http://www.exploit-db.com/exploits/17696
url: http://packetstormsecurity.org/files/view/104441
url: http://marc.info/?l=apache-httpd-dev&m=131420013520206&w=2
url: http://mail-archives.apache.org/mod_mbox/httpd-dev/201108.mbox/%3CCAAPSnn2P
↪0-d-C4nQt_TES2RRWiZr7urefhTKPWBC1b+K1Dqc7g@mail.gmail.com%3E
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-0856
dfn-cert: DFN-CERT-2012-0746
dfn-cert: DFN-CERT-2012-0731
dfn-cert: DFN-CERT-2011-1726
dfn-cert: DFN-CERT-2011-1725
dfn-cert: DFN-CERT-2011-1693
dfn-cert: DFN-CERT-2011-1692
dfn-cert: DFN-CERT-2011-1632
dfn-cert: DFN-CERT-2011-1631
dfn-cert: DFN-CERT-2011-1593
dfn-cert: DFN-CERT-2011-1519
dfn-cert: DFN-CERT-2011-1492
dfn-cert: DFN-CERT-2011-1440
dfn-cert: DFN-CERT-2011-1435
dfn-cert: DFN-CERT-2011-1430
dfn-cert: DFN-CERT-2011-1429
dfn-cert: DFN-CERT-2011-1425
dfn-cert: DFN-CERT-2011-1379
dfn-cert: DFN-CERT-2011-1362
dfn-cert: DFN-CERT-2011-1343
dfn-cert: DFN-CERT-2011-1342
dfn-cert: DFN-CERT-2011-1341
dfn-cert: DFN-CERT-2011-1335
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-1333
dfn-cert: DFN-CERT-2011-1318
dfn-cert: DFN-CERT-2011-1312
dfn-cert: DFN-CERT-2011-1298
```

High (CVSS: 7.5)
NVT: Joomla < 3.9.5 Multiple Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

Joomla! is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.9.5
Installation
path / port:       /joomla
```

Impact

Successful exploitation would allow an attacker to access sensitive information or execute arbitrary commands.

Solution

Solution type: VendorFix
Update to version 3.9.5.

Affected Software/OS

Joomla! through version 3.9.4.

Vulnerability Insight

The following vulnerabilities exist:

- The Media Manager component does not properly sanitize the folder parameter, allowing attackers to act outside the media manager root directory
- The 'refresh list of helpsites' endpoint of com_users lacks access checks, allowing calls from unauthenticated users
- The $.extend method of JQuery is vulnerable to Object.prototype pollution attacks (CVE-2019-11358)

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Joomla < 3.9.5 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.113369

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2019-10945
cve: CVE-2019-10946
cve: CVE-2019-11358
url: https://developer.joomla.org/security-centre/777-20190401-core-directory-tr
↪aversal-in-com-media
url: https://developer.joomla.org/security-centre/778-20190402-core-helpsites-re
↪fresh-endpoint-callable-for-unauthenticated-users
url: https://developer.joomla.org/security-centre.html
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K20/0800
cert-bund: CB-K20/0710
cert-bund: CB-K20/0324
cert-bund: CB-K20/0314
cert-bund: CB-K20/0309
cert-bund: CB-K20/0106
cert-bund: CB-K20/0041
cert-bund: CB-K20/0037
cert-bund: CB-K20/0034
cert-bund: CB-K19/0921
cert-bund: CB-K19/0920
cert-bund: CB-K19/0916
cert-bund: CB-K19/0911
cert-bund: CB-K19/0909
cert-bund: CB-K19/0619
cert-bund: CB-K19/0504
cert-bund: CB-K19/0287
dfn-cert: DFN-CERT-2020-2423
dfn-cert: DFN-CERT-2020-2335
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-2130
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1574
dfn-cert: DFN-CERT-2020-1537
dfn-cert: DFN-CERT-2020-1506
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0769
dfn-cert: DFN-CERT-2020-0721
dfn-cert: DFN-CERT-2020-0276
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0102
dfn-cert: DFN-CERT-2020-0100
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-2156
dfn-cert: DFN-CERT-2019-2126
dfn-cert: DFN-CERT-2019-1861
dfn-cert: DFN-CERT-2019-1663
dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1182
dfn-cert: DFN-CERT-2019-1153
dfn-cert: DFN-CERT-2019-1118
dfn-cert: DFN-CERT-2019-1033
dfn-cert: DFN-CERT-2019-0914
dfn-cert: DFN-CERT-2019-0899
dfn-cert: DFN-CERT-2019-0805
dfn-cert: DFN-CERT-2019-0723
```

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

Product detection result

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary

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

Vulnerability Detection Result

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

Impact

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

Solution

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

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

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

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: CVE-2010-1134
cve: CVE-2010-1133
cve: CVE-2010-1136
bid: 38608
url: http://www.securityfocus.com/bid/38608
url: http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=24734
url: http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25046
url: http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25424
url: http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25435
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: Joomla! Prior to 1.6.1 Multiple Security Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

Joomla! is prone to multiple security vulnerabilities including:
- An SQL-injection issue
- A path-disclosure vulnerability
- Multiple cross-site scripting issues
- Multiple information-disclosure vulnerabilities
- A URI-redirection vulnerability
- A security-bypass vulnerability
- A cross-site request-forgery vulnerability
- A denial-of-service vulnerability

Vulnerability Detection Result

```
Installed version: 1.5.15
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     1.6.1
```

Impact

An attacker can exploit these vulnerabilities to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, steal cookie-based authentication credentials, disclose or modify sensitive information, exploit latent vulnerabilities in the underlying database, deny service to legitimate users, redirect a victim to a potentially malicious site, or perform unauthorized actions. Other attacks are also possible.

Solution

Solution type: VendorFix

The vendor released a patch. Please see the references for more information.

Affected Software/OS

Versions prior to Joomla! 1.6.1 are vulnerable.

Vulnerability Detection Method

Details: `Joomla! Prior to 1.6.1 Multiple Security Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.103114

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`

Method: `joomla Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
bid: 46787
url: https://www.securityfocus.com/bid/46787
url: http://www.joomla.org/announcements/release-news/5350-joomla-161-released.h
↪tml
```

High (CVSS: 7.5)

NVT: phpinfo() output Reporting

Summary

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

Vulnerability Detection Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
https://owasp/bWAPP/phpinfo.php
https://owasp/mutillidae/phpinfo.php
https://owasp/vicnum/test.php
https://owasp/vicnum/test.php?mode=phpinfo
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

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

High (CVSS: 7.5)
NVT: Joomla! < 3.9.7 Multiple Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

Joomla! is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.9.7
Installation
path / port:       /joomla
```

Impact

Successful exploitation can have effects ranging from disclosure of sensitive information to executing arbitrary code on the target machine.

Solution

Solution type: VendorFix
Update to version 3.9.7.

Affected Software/OS

Joomla! through version 3.9.6.

Vulnerability Insight

The following vulnerabilities exist:
- The update server URL of com_joomlaupdate can be manipulated by non Super-Admin users.

. . . continues on next page . . .

. . . continued from previous page . . .

- The subform fieldtype does not sufficiently filter or validate input of subfields. This leads to XSS attack vectors.
- The CSV export of com_actionslogs is vulnerable to CSV injection.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! < 3.9.7 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.113390

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2019-12764
cve: CVE-2019-12765
cve: CVE-2019-12766
bid: 108729
bid: 108735
bid: 108736
url: https://developer.joomla.org/security-centre/785-20190603-core-acl-hardenin
↪g-of-com-joomlaupdate
url: https://developer.joomla.org/security-centre/783-20190601-core-csv-injectio
↪n-in-com-actionlogs
url: https://developer.joomla.org/security-centre/784-20190602-core-xss-in-subfo
↪rm-field
cert-bund: CB-K19/0495
dfn-cert: DFN-CERT-2019-1179
```

High (CVSS: 7.5)
NVT: WordPress Spreadsheet plugin Multiple Vulnerabilities

Product detection result

```
cpe:/a:wordpress:wordpress:2.0
Detected by WordPress Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900182)
```

Summary
This host is installed with WordPress Spreadsheet plugin and is prone to multiple vulnerabilities.

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

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote attackers to execute arbitrary HTML and script code in a users browser session in the context of an affected site and inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.

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.

Affected Software/OS
WordPress Spreadsheet plugin version 0.62

Vulnerability Insight
Input passed via the 'ss_id' parameter to wpSS/ss_handler.php script is not validated before returning it to users.

Vulnerability Detection Method
Send a crafted data via HTTP GET request and check whether it is able to read cookie or not.
Details: `WordPress Spreadsheet plugin Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.804872

Product Detection Result
Product: `cpe:/a:wordpress:wordpress:2.0`
Method: `WordPress Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900182)

References

```
cve: CVE-2014-8363
cve: CVE-2014-8364
bid: 69073
bid: 69089
url: http://packetstormsecurity.com/files/127770
```

High (CVSS: 7.5)
NVT: Joomla! < 3.8.12 Multiple Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary
This host is running Joomla and is prone to multiple vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 1.5.15
Fixed version:     3.8.12
Installation
path / port:       /joomla
```

Solution
Solution type: VendorFix
Upgrade to version 3.8.12 or later.

Affected Software/OS
Joomla! CMS versions 1.5.0 through 3.8.11

Vulnerability Insight
The following vulnerabilities exist:
- Inadequate output filtering on the user profile page could lead to a stored XSS attack. (CVE-2018-15880)
- Inadequate checks in the InputFilter class could allow specifically prepared PHAR files to pass the upload filter. (CVE-2018-15882)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! < 3.8.12 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.112371

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2018-15880
cve: CVE-2018-15882
url: https://developer.joomla.org/security-centre/744-20180802-core-stored-xss-v
↪ulnerability-in-the-frontend-profile.html
url: https://developer.joomla.org/security-centre/743-20180801-core-hardening-th
↪e-inputfilter-for-phar-stubs.html
dfn-cert: DFN-CERT-2018-1744
```

[return to 10.0.2.4]

2.1.5 Medium 8080/tcp

Medium (CVSS: 6.8)
NVT: Apache Tomcat servlet/JSP container default files

Product detection result

```
cpe:/a:apache:tomcat:6.0.24
Detected by Apache Tomcat Detection (Consolidation) (OID: 1.3.6.1.4.1.25623.1.0.
↪107652)
```

Summary

The Apache Tomcat servlet/JSP container has default files installed.

Vulnerability Detection Result

```
The following default files were found :
http://owasp:8080/examples/servlets/index.html
http://owasp:8080/examples/jsp/snp/snoop.jsp
http://owasp:8080/examples/jsp/index.html
```

Impact

These files should be removed as they may help an attacker to guess the exact version of the Apache Tomcat which is running on this host and may provide other useful information.

Solution

Solution type: Mitigation

Remove default files, example JSPs and Servlets from the Tomcat Servlet/JSP container.

Vulnerability Insight

Default files, such as documentation, default Servlets and JSPs were found on the Apache Tomcat servlet/JSP container.

Vulnerability Detection Method

Details: `Apache Tomcat servlet/JSP container default files`
OID:1.3.6.1.4.1.25623.1.0.12085

Product Detection Result

Product: `cpe:/a:apache:tomcat:6.0.24`
Method: `Apache Tomcat Detection (Consolidation)`
OID: 1.3.6.1.4.1.25623.1.0.107652)

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
The following URLs requires Basic Authentication (URL:realm name):
http://owasp:8080/host-manager/html:"Tomcat Host Manager Application"
http://owasp:8080/manager/html:"Tomcat Manager Application"
http://owasp:8080/manager/status:"Tomcat Manager Application"
```

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

References

```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

[return to 10.0.2.4]

2.1.6 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: Joomla! <= 3.9.19 Multiple Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Joomla! is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.9.20
Installation
path / port:       /joomla
```

Impact
Successful exploitation would allow an attacker to read sensitive information, inject arbitrary HTML and JavaScript into the site or perform actions in the context of another use.

Solution
Solution type: VendorFix
Update to version 3.9.20.

Affected Software/OS
Joomla! through version 3.9.19.

Vulnerability Insight
The following vulnerabilities exist:
- A missing token check in the remove request section of com_privacy causes a CSRF vulnerability. (CVE-2020-15695)
- Lack of input filtering and escaping allows XSS attacks in mod_random_image. (CVE-2020-15696)
- Internal read-only fields in the User table class could be modified by users. (CVE-2020-15697)
- Inadequate filtering on the system information screen could expose Redis or proxy credentials. (CVE-2020-15698)
- Missing validation checks on the usergroups table object can result in a broken site configuration. (CVE-2020-15699)
- A missing token check in the ajax_install endpoint of com_installer causes a CSRF vulnerability. (CVE-2020-15700)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! <= 3.9.19 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.113726

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-15695
cve: CVE-2020-15696
cve: CVE-2020-15697
cve: CVE-2020-15698
cve: CVE-2020-15699
cve: CVE-2020-15700
url: https://developer.joomla.org/security-centre/820-20200703-core-csrf-in-com-
↪privacy-remove-request-feature.html
url: https://developer.joomla.org/security-centre/822-20200705-core-escape-mod-r
↪andom-image-link.html
url: https://developer.joomla.org/security-centre/821-20200704-core-variable-tam
↪pering-via-user-table-class.html
url: https://developer.joomla.org/security-centre/823-20200706-core-system-infor
↪mation-screen-could-expose-redis-or-proxy-credentials.html
url: https://developer.joomla.org/security-centre/819-20200702-core-missing-chec
↪ks-can-lead-to-a-broken-usergroups-table-record.html
url: https://developer.joomla.org/security-centre/818-20200701-core-csrf-in-com-
↪installer-ajax-install-endpoint.html
cert-bund: CB-K20/0716
dfn-cert: DFN-CERT-2020-1517
```

Medium (CVSS: 6.8)
NVT: Joomla! < 3.9.13 Multiple Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

Joomla! is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.9.13
Installation
path / port:       /joomla
```

Impact

Successful exploitation would allow an attacker to access sensitive information or perform actions in the context of another user.

Solution

Solution type: VendorFix

Update to version 3.9.13.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Joomla! through version 3.9.12.

Vulnerability Insight

The following vulnerabilities exist:

- A missing check in com_template causes a CSRF vulnerability.
- A missing access check in the phputf8 mapping files could lead to a path disclosure.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Joomla! < 3.9.13 Multiple Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.113556

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`

Method: `joomla Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2019-18650
cve: CVE-2019-18674
url: https://developer.joomla.org/security-centre/794-20191001-core-csrf-in-com-
↪template-overrides-view.html
url: https://developer.joomla.org/security-centre/795-20191002-core-path-disclos
↪ure-in-phpuft8-mapping-files.html
cert-bund: CB-K19/0960
dfn-cert: DFN-CERT-2019-2299
```

Medium (CVSS: 6.8)
NVT: WebCalendar Multiple CSS and CSRF Vulnerabilities

Summary

The host is running WebCalendar and is prone to multiple CSS and CSRF Vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.0.3
Vulnerable range:  Less than or equal to 1.2.0
```

Impact

Successful exploitation could allow attackers to conduct cross-site scripting and request forgery attacks.

Solution

Solution type: VendorFix

Upgrade to WebCalendar version 1.2.1 or later.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

WebCalendar version 1.2.0 and prior.

Vulnerability Insight

- Input passed to the 'tab' parameter in 'users.php' is not properly sanitised before being returned to the user.
- Input appended to the URL after 'day.php', 'month.php', and 'week.php' is not properly sanitised before being returned to the user.
- The application allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to delete an event, ban an IP address from posting, or change the administrative password if a logged-in administrative user visits a malicious web site.

Vulnerability Detection Method

Details: `WebCalendar Multiple CSS and CSRF Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800472

References

```
cve: CVE-2010-0636
cve: CVE-2010-0637
cve: CVE-2010-0638
bid: 38053
url: http://secunia.com/advisories/38222
url: http://holisticinfosec.org/content/view/133/45/
```

Medium (CVSS: 6.5)
NVT: Joomla! < 3.8.13 ACL Violation Vulnerability

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

If an attacker gets access to the mail account of an user who can approve admin verifications in the registration process, he can activate himself.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.8.13
Installation
path / port:       /joomla
```

Solution

Solution type: VendorFix
Update to version 3.8.13 or later.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Joomla! CMS versions 1.5.0 through 3.8.12.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! < 3.8.13 ACL Violation Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141580

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2018-17855
url: https://developer.joomla.org/security-centre/754-20181004-core-acl-violatio
↪n-in-com-users-for-the-admin-verification
dfn-cert: DFN-CERT-2018-2061
```

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)
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
url: https://blog.ripstech.com/2018/scan-verify-patch-security-issues-in-minutes
↪/
```

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.

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

References

```
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
bid: 9506
bid: 9561
bid: 11604
bid: 15222
bid: 19915
bid: 24456
bid: 33374
bid: 36956
bid: 36990
bid: 37995
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
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

Medium (CVSS: 5.0)
NVT: MacOS X Finder '.DS_Store' Information Disclosure

Summary
MacOS X creates a hidden file '.DS_Store', in each directory that has been viewed with the 'Finder'. This file contains a list of the contents of the directory, giving an attacker information on the structure and contents of your website.

Vulnerability Detection Result

```
The following files were identified:
http://owasp/cyclone/.DS_Store
```

Solution
Solution type: Workaround
Block access to hidden files (starting with a dot) within your webservers configuration

Vulnerability Detection Method
Details: `MacOS X Finder '.DS_Store' Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.10756

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2016-1776
cve: CVE-2018-6470
bid: 3316
bid: 3324
bid: 85054
url: https://www.securityfocus.com/bid/3316
url: https://www.securityfocus.com/bid/3324
url: https://www.securityfocus.com/bid/85054
url: https://helpx.adobe.com/dreamweaver/kb/remove-ds-store-files-mac.html
url: https://support.apple.com/en-us/HT1629
cert-bund: CB-K16/0450
dfn-cert: DFN-CERT-2016-0489
```

Medium (CVSS: 5.0)
NVT: Joomla! Core LDAP Information Disclosure Vulnerability Nov17

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.8.2
```

Impact

Successfully exploiting this issue allow remote attackers to disclose username and password.

Solution

Solution type: VendorFix

Upgrade to Joomla version 3.8.2 or later.

Affected Software/OS

Joomla core version 1.5.0 through 3.8.1

Vulnerability Insight

The flaw exists due to an inadequate escaping in the LDAP authentication plugin.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Joomla! Core LDAP Information Disclosure Vulnerability Nov17`

OID:1.3.6.1.4.1.25623.1.0.811896

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2017-14596
bid: 100898
url: https://developer.joomla.org/security-centre/714-20171101-core-ldap-informa
↪tion-disclosure.html
url: https://blog.ripstech.com/2017/joomla-takeover-in-20-seconds-with-ldap-inje
↪ction-cve-2017-14596
cert-bund: CB-K17/1899
cert-bund: CB-K17/1591
dfn-cert: DFN-CERT-2017-1977
dfn-cert: DFN-CERT-2017-1663
```

Medium (CVSS: 5.0)
NVT: Source Control Management (SCM) Files Accessible

Summary

The script attempts to identify files of a SCM accessible at the webserver.

Vulnerability Detection Result

```
The following SCM files/folders were identified:
http://owasp/zapwave/.svn/wc.db
http://owasp/mutillidae/.git/logs/HEAD
http://owasp/mutillidae/.git/config
http://owasp/mutillidae/.git/description
http://owasp/mutillidae/.git/FETCH_HEAD
http://owasp/mutillidae/.git/ORIG_HEAD
http://owasp/mutillidae/.git/HEAD
http://owasp/MCIR/.git/logs/HEAD
http://owasp/MCIR/.git/config
http://owasp/MCIR/.git/description
http://owasp/MCIR/.git/FETCH_HEAD
http://owasp/MCIR/.git/ORIG_HEAD
http://owasp/MCIR/.git/HEAD
http://owasp/dvwa/.git/logs/HEAD
http://owasp/dvwa/.git/config
http://owasp/dvwa/.git/description
http://owasp/dvwa/.git/FETCH_HEAD
http://owasp/dvwa/.git/ORIG_HEAD
http://owasp/dvwa/.git/HEAD
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Based on the information provided in this files an attacker might be able to gather additional info about the structure of the system and its applications.

Solution

Solution type: Mitigation

Restrict access to the Admin Pages for authorized systems only.

Vulnerability Insight

Currently the script is checking for files of the following SCM:
- Git (.git)
- Mercurial (.hg)
- Bazaar (.bzr)
- CVS (CVS/Root, CVS/Entries)
- Subversion (.svn)

Vulnerability Detection Method

Check the response if SCM files are accessible.

Details: `Source Control Management (SCM) Files Accessible`

OID:1.3.6.1.4.1.25623.1.0.111084

References

```
url: http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-be
↪long-to-us
url: https://github.com/anantshri/svn-extractor
url: https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d
url: https://blog.netspi.com/dumping-git-data-from-misconfigured-web-servers/
url: http://resources.infosecinstitute.com/hacking-svn-git-and-mercurial/
```

Medium (CVSS: 5.0)

NVT: Joomla! < 3.8.0 LDAP Information Disclosure Vulnerability

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.8.0
```

Impact

Successfully exploiting these issues will allow remote attackers to gain access to potentially sensitive information.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: VendorFix

Upgrade to Joomla version 3.8.0 or later.

Affected Software/OS

Joomla! versions 1.5.0 through 3.7.5

Vulnerability Insight

Joomla is prone to the following information disclosure vulnerability:

- Inadequate escaping in the LDAP authentication plugin can result into a disclosure of username and password.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Joomla! < 3.8.0 LDAP Information Disclosure Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.112049

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`

Method: `joomla Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2017-14596
url: https://developer.joomla.org/security-centre/711-20170902-core-ldap-informa
↪tion-disclosure
cert-bund: CB-K17/1899
cert-bund: CB-K17/1591
dfn-cert: DFN-CERT-2017-1977
dfn-cert: DFN-CERT-2017-1663
```

Medium (CVSS: 5.0)

NVT: Joomla! Information Disclosure and Cross-Site Scripting Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to information disclosure and cross-site scripting vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     3.7.0
```

Impact
Successfully exploiting these issues allow remote attackers to gain access to potentially sensitive information and conduct cross-site scripting attacks.

Solution
Solution type: VendorFix
Upgrade to Joomla version 3.7.0 or later.

Affected Software/OS
Joomla core versions 1.5.0 through 3.6.5

Vulnerability Insight
Multiple flaws are due to,
- Mail sent using the JMail API leaked the used PHPMailer version in the mail headers.
- Inadequate filtering of specific HTML attributes.
- Inadequate filtering of multibyte characters.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! Information Disclosure and Cross-Site Scripting Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.811042

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References
```
cve: CVE-2017-7983
cve: CVE-2017-7986
cve: CVE-2017-7985
bid: 98016
bid: 98024
bid: 98020
url: https://developer.joomla.org/security-centre/686-20170404-core-xss-vulnerab
↪ility
url: https://developer.joomla.org/security-centre/685-20170403-core-xss-vulnerab
↪ility
url: https://developer.joomla.org/security-centre/683-20170401-core-information-
↪disclosure
cert-bund: CB-K17/1113
cert-bund: CB-K17/0698
dfn-cert: DFN-CERT-2017-1151
dfn-cert: DFN-CERT-2017-0720
```

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

Product detection result

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary

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

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     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

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
url: http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-r
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪eleased
url: https://sourceforge.net/p/tikiwiki/code/60308/
url: https://tiki.org
```

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

Product detection result

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary

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

Vulnerability Detection Result

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

Impact

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

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

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2008-5318
cve: CVE-2008-5319
url: http://secunia.com/advisories/32341
url: http://info.tikiwiki.org/tiki-read_article.php?articleId=41
```

Medium (CVSS: 5.0)
NVT: WebCalendar User Account Enumeration Disclosure Issue

Summary
The version of WebCalendar on the remote host is prone to a user account enumeration weakness in that in response to login attempts it returns different error messages depending on whether the user exists or the password is invalid.

Vulnerability Detection Result

```
Vulnerable URL: http://owasp/webcal/login.php
```

Solution
Solution type: VendorFix
Upgrade to WebCalendar 1.0.4 or later.

Vulnerability Detection Method
Details: `WebCalendar User Account Enumeration Disclosure Issue`
OID:1.3.6.1.4.1.25623.1.0.80021

References

```
cve: CVE-2006-2247
bid: 17853
osvdb: 25280
url: http://www.securityfocus.com/archive/1/433053/30/0/threaded
url: http://www.securityfocus.com/archive/1/436263/30/0/threaded
url: http://sourceforge.net/project/shownotes.php?group_id=3870&release_id=42301
↪0
```

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

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

Vulnerability Detection Result

```
Vulnerable URL: http://owasp/mutillidae/index.php?page=/etc/passwd
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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.

Affected Software/OS

awiki 20100125 is vulnerable. Other versions may also be affected.

Vulnerability Detection Method

Details: `awiki Multiple Local File Include Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.103210

References

```
bid: 49187
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://owasp/AppSensorDemo/login.jsp:password
http://owasp/bodgeit/login.jsp:password
http://owasp/cyclone/signin:session[password]
http://owasp/cyclone/signup:user[password]
http://owasp/ghost/:pass
http://owasp/phpmyadmin/:pma_password
http://owasp/phpmyadmin/?D=A:pma_password
http://owasp/railsgoat/:password
http://owasp/railsgoat/?D=A:password
http://owasp/railsgoat:password
http://owasp/shepherd/login.jsp:pwd
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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

References

```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_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: Joomla! Core 'Media Manager' XSS Vulnerability (20180509)

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to a cross site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.8.8
Installation
path / port:       /joomla
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote attackers to conduct XSS attack.

Solution

Solution type: VendorFix

Upgrade to Joomla version 3.8.8 or later. Please see the references for more information.

Affected Software/OS

Joomla core versions 1.5.0 through 3.8.7

Vulnerability Insight

The flaw exists due to inadequate filtering of file and folder names in media manager.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Joomla! Core 'Media Manager' XSS Vulnerability (20180509)`

OID:1.3.6.1.4.1.25623.1.0.813406

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`

Method: `joomla Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2018-6378
url: https://developer.joomla.org/security-centre/737-20180509-core-xss-vulnerab
↪ility-in-the-media-manager.html
dfn-cert: DFN-CERT-2018-0979
```

Medium (CVSS: 4.3)

NVT: Joomla! Core Cross-Site Scripting Vulnerability - July17

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to cross-site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.7.4
```

Impact

Successfully exploiting this issue will allow remote attacker to conduct cross-site scripting attacks.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Solution type: VendorFix
Upgrade to Joomla version 3.7.4 or later.

Affected Software/OS
Joomla core versions 1.5.0 through 3.7.3

Vulnerability Insight
The flaw exists due to Inadequate filtering of potentially malicious HTML tags in various components of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! Core Cross-Site Scripting Vulnerability - July17`
OID:1.3.6.1.4.1.25623.1.0.811257

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References
```
cve: CVE-2017-11612
url: https://developer.joomla.org/security-centre/701-20170704-core-installer-la
↪ck-of-ownership-verification
cert-bund: CB-K17/1245
dfn-cert: DFN-CERT-2017-1286
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Product detection result
```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Result
```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:        /mutillidae/javascript/ddsmoothmenu
```

Solution
Solution type: VendorFix
Update to version 1.6.3 or later or apply the patch.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary
jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

```
Installed version: 1.8.2
Fixed version:     1.9.0
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:        /owaspbricks/config/../javascripts
```

Solution
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References
```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Product detection result
```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Result
```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
path / port:        /
```

Solution
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update to version 1.6.3 or later or apply the patch.

Affected Software/OS

jQuery prior to version 1.6.3.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /mutillidae/javascript/ddsmoothmenu
```

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary
jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

```
Installed version: 1.8.0
Fixed version:     1.9.0
Installation
path / port:       /cyclone/assets
```

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 4.3)
NVT: OrangeHRM 'jobVacancy.php' Cross Site Scripting Vulnerability

Product detection result

```
cpe:/a:orangehrm:orangehrm:2.4.2
Detected by OrangeHRM Detection (OID: 1.3.6.1.4.1.25623.1.0.100850)
```

Summary
OrangeHRM is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input before using it in dynamically generated content.

Vulnerability Detection Result

```
Vulnerable URL: http://owasp/orangehrm/templates/recruitment/jobVacancy.php?recr
↪uitcode=</script><script>alert('vt-xss-test')</script>
```

Impact
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks.

Solution
Solution type: WillNotFix

. . . continues on next page . . .

. . . continued from previous page . . .

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.

Affected Software/OS
OrangeHRM 2.6.2 is vulnerable. Other versions may also be affected.

Vulnerability Detection Method
Details: `OrangeHRM 'jobVacancy.php' Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103132

Product Detection Result
Product: `cpe:/a:orangehrm:orangehrm:2.4.2`
Method: `OrangeHRM Detection`
OID: 1.3.6.1.4.1.25623.1.0.100850)

References

```
bid: 47046
url: https://www.securityfocus.com/bid/47046
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary
jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /
```

Solution
Solution type: VendorFix

. . . continues on next page . . .

... continued from previous page ...

Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2020-0590
```

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

Product detection result

```
cpe:/a:phpmyadmin:phpmyadmin:3.3.2 -
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.

... continues on next page ...

. . . continued from previous page . . .

Affected Software/OS

phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight

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

Vulnerability Detection Method

Details: `phpMyAdmin 'error.php' Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801660

Product Detection Result

Product: `cpe:/a:phpmyadmin:phpmyadmin:3.3.2 -`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
cve: CVE-2010-4480
url: http://www.exploit-db.com/exploits/15699/
url: http://www.vupen.com/english/advisories/2010/3133
dfn-cert: DFN-CERT-2011-0467
dfn-cert: DFN-CERT-2011-0451
dfn-cert: DFN-CERT-2011-0016
dfn-cert: DFN-CERT-2011-0002
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

```
Installed version: 1.8.2
Fixed version:     1.9.0
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:        /owaspbricks/javascripts
```

Solution

Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 4.3)
NVT: Tiki Wiki CMS Groupware Multiple Cross Site Scripting Vulnerabilities

Product detection result

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary

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

Vulnerability Detection Result

```
Vulnerable URL: http://owasp/tikiwiki/tiki-listpages.php/<script>alert("XSS_Chec
↪k");</script>
```

Impact

. . . continues on next page . . .

... continued from previous page ...

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

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
bid: 34106
bid: 34107
bid: 34108
url: http://secunia.com/advisories/34273
url: http://info.tikiwiki.org/tiki-read_article.php?articleId=51
```

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

... continues on next page ...

. . . continued from previous page . . .

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

References

```
cve: CVE-2012-0053
bid: 51706
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.html
cert-bund: CB-K15/0080
cert-bund: CB-K14/1505
cert-bund: CB-K14/0608
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2014-1592
dfn-cert: DFN-CERT-2014-0635
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-0928
dfn-cert: DFN-CERT-2012-0758
dfn-cert: DFN-CERT-2012-0744
dfn-cert: DFN-CERT-2012-0568
dfn-cert: DFN-CERT-2012-0425
dfn-cert: DFN-CERT-2012-0424
dfn-cert: DFN-CERT-2012-0387
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
dfn-cert: DFN-CERT-2012-0306
dfn-cert: DFN-CERT-2012-0264
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188
```

Medium (CVSS: 4.3)
NVT: Joomla! Multiple Cross-site Scripting Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to multiple Cross-site scripting vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     1.5.21
```

Impact

Successful exploitation will allow attackers to inject arbitrary web script or HTML via vectors involving 'multiple encoded entities'.

Solution

Solution type: VendorFix

Upgrade to Joomla! 1.5.21 or later.

Affected Software/OS

Joomla! versions 1.5.x before 1.5.21

Vulnerability Insight

The flaws are due to inadequate filtering of multiple encoded entities, which could be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser in the security context of an affected Web site.

Vulnerability Detection Method

Details: `Joomla! Multiple Cross-site Scripting Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.901168

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`

Method: `joomla Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2010-3712
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.vupen.com/english/advisories/2010/2615
url: http://developer.joomla.org/security/news/9-security/10-core-security/322-2
↪0101001-core-xss-vulnerabilities
```

Medium (CVSS: 4.3)
NVT: Joomla! 'Uri' class XSS Vulnerability

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to cross site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.8.4
Installation
path / port:       /joomla
```

Impact

Successfully exploiting this issue will allow remote attackers to execute arbitrary javascript code in the context of current user.

Solution

Solution type: VendorFix

Upgrade to Joomla version 3.8.4 or later.

Affected Software/OS

Joomla core version 1.5.0 through 3.8.3

Vulnerability Insight

The flaw exists due to inadequate input filtering in the Uri class (formerly JUri).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Joomla! 'Uri' class XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.812681

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2018-6379
url: https://developer.joomla.org/security-centre/721-20180104-core-xss-vulnerab
↪ility.html
cert-bund: CB-K18/0197
dfn-cert: DFN-CERT-2018-0214
```

Medium (CVSS: 4.3)
NVT: Tiki Wiki CMS Groupware < 21.0 XSS 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

Tiki Wiki is prone to a cross-site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     21.0
Installation
path / port:       /tikiwiki
```

Solution

Solution type: VendorFix

Update to version 21.0.

Affected Software/OS

Tiki Wiki CMS Groupware version 20.0 and prior.

Vulnerability Insight

Some php pages receive input from an upstream component, but do not neutralize or incorrectly neutralize special characters such as '<', '>', and '&'. These characters could be interpreted as web-scripting elements when they are sent to a downstream component that processes web pages.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Tiki Wiki CMS Groupware < 21.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.112721

Product Detection Result

Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`

Method: `Tiki Wiki CMS Groupware Version Detection`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.901001)

References

```
cve: CVE-2020-8966
url: https://www.incibe-cert.es/en/early-warning/security-advisories/cross-site-
↪scripting-xss-flaws-found-tiki-wiki-cms-software
```

Medium (CVSS: 4.3)
NVT: Tiki Wiki < 21.2 XSS 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

Tiki Wiki is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     21.2
Installation
path / port:       /tikiwiki
```

Impact

Successful exploitation would allow an attacker to inject arbitrary HTML and JavaScript into the site.

Solution

Solution type: VendorFix

Update to version 21.2.

Affected Software/OS

Tiki Wiki through version 21.1.

Vulnerability Insight

The vulnerability exists because some patterns are not properly considered in lib/core/TikiFilter/PreventXss.php.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Tiki Wiki < 21.2 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.113737

. . . continues on next page . . .

. . . continued from previous page . . .

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-2020-16131
url: https://gitlab.com/tikiwiki/tiki/-/commit/d12d6ea7b025d3b3f81c8a71063fe9f89
↪e0c4bf1
```

Medium (CVSS: 4.3)
NVT: WebCalendar Multiple Cross Site Scripting Vulnerabilities

Summary

This host is running WebCalendar and is prone to multiple cross site scripting vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.0.3
Vulnerable range:  Less than or equal to 1.2.3
```

Impact

Successful exploitation could allow remote attackers to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Solution

Solution type: VendorFix
Upgrade to WebCalendar versions 1.2.4 or later.

Affected Software/OS

WebCalendar versions 1.2.3 and prior.

Vulnerability Insight

The flaws are caused by improper validation of user-supplied input in various scripts, which allows attackers to execute arbitrary HTML and script code on the web server.

Vulnerability Detection Method

Details: `WebCalendar Multiple Cross Site Scripting Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.802305

References

```
url: http://packetstormsecurity.org/files/view/102785/SSCHADV2011-008.txt
```

Medium (CVSS: 4.3)
NVT: Apache Web Server ETag Header Information Disclosure Weakness

Product detection result

```
cpe:/a:apache:http_server:2.2.14
Detected by Apache HTTP/Web Server Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.
↪900498)
```

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: 286483
Size: 28067
```

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

Product Detection Result

Product: `cpe:/a:apache:http_server:2.2.14`

Method: `Apache HTTP/Web Server Detection (HTTP)`

OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
cve: CVE-2003-1418
bid: 6939
url: https://www.securityfocus.com/bid/6939
url: http://httpd.apache.org/docs/mod/core.html#fileetag
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.openbsd.org/errata32.html
url: http://support.novell.com/docs/Tids/Solutions/10090670.html
cert-bund: CB-K17/1750
cert-bund: CB-K17/0896
cert-bund: CB-K15/0469
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-0925
dfn-cert: DFN-CERT-2015-0495
```

[return to 10.0.2.4]

2.1.7 Medium 8081/tcp

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

```
Installed version: 1.7.2
Fixed version:     1.9.0
Installation
path / port:       /admin/../js
```

Solution

Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.141636

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2020-0590
```

[return to 10.0.2.4]

2.1.8 Medium 22/tcp

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary

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

Vulnerability Detection Result

```
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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

References

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

[return to 10.0.2.4]

2.1.9 Medium 443/tcp

Medium (CVSS: 6.8)

NVT: Joomla! < 3.9.13 Multiple Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

Joomla! is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.9.13
Installation
path / port:       /joomla
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation would allow an attacker to access sensitive information or perform actions in the context of another user.

Solution
Solution type: VendorFix
Update to version 3.9.13.

Affected Software/OS
Joomla! through version 3.9.12.

Vulnerability Insight
The following vulnerabilities exist:
- A missing check in com_template causes a CSRF vulnerability.
- A missing access check in the phputf8 mapping files could lead to a path disclosure.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! < 3.9.13 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.113556

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2019-18650
cve: CVE-2019-18674
url: https://developer.joomla.org/security-centre/794-20191001-core-csrf-in-com-
↪template-overrides-view.html
url: https://developer.joomla.org/security-centre/795-20191002-core-path-disclos
↪ure-in-phpuft8-mapping-files.html
cert-bund: CB-K19/0960
dfn-cert: DFN-CERT-2019-2299
```

Medium (CVSS: 6.8)
NVT: Joomla! <= 3.9.19 Multiple Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Joomla! is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.9.20
Installation
path / port:       /joomla
```

Impact

Successful exploitation would allow an attacker to read sensitive information, inject arbitrary HTML and JavaScript into the site or perform actions in the context of another use.

Solution

Solution type: VendorFix

Update to version 3.9.20.

Affected Software/OS

Joomla! through version 3.9.19.

Vulnerability Insight

The following vulnerabilities exist:

- A missing token check in the remove request section of com_privacy causes a CSRF vulnerability. (CVE-2020-15695)
- Lack of input filtering and escaping allows XSS attacks in mod_random_image. (CVE-2020-15696)
- Internal read-only fields in the User table class could be modified by users. (CVE-2020-15697)
- Inadequate filtering on the system information screen could expose Redis or proxy credentials. (CVE-2020-15698)
- Missing validation checks on the usergroups table object can result in a broken site configuration. (CVE-2020-15699)
- A missing token check in the ajax_install endpoint of com_installer causes a CSRF vulnerability. (CVE-2020-15700)

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Joomla! <= 3.9.19 Multiple Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.113726

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`

Method: `joomla Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2020-15695
cve: CVE-2020-15696
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-15697
cve: CVE-2020-15698
cve: CVE-2020-15699
cve: CVE-2020-15700
url: https://developer.joomla.org/security-centre/820-20200703-core-csrf-in-com-
↪privacy-remove-request-feature.html
url: https://developer.joomla.org/security-centre/822-20200705-core-escape-mod-r
↪andom-image-link.html
url: https://developer.joomla.org/security-centre/821-20200704-core-variable-tam
↪pering-via-user-table-class.html
url: https://developer.joomla.org/security-centre/823-20200706-core-system-infor
↪mation-screen-could-expose-redis-or-proxy-credentials.html
url: https://developer.joomla.org/security-centre/819-20200702-core-missing-chec
↪ks-can-lead-to-a-broken-usergroups-table-record.html
url: https://developer.joomla.org/security-centre/818-20200701-core-csrf-in-com-
↪installer-ajax-install-endpoint.html
cert-bund: CB-K20/0716
dfn-cert: DFN-CERT-2020-1517
```

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)
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
url: https://blog.ripstech.com/2018/scan-verify-patch-security-issues-in-minutes
↪/
```

Medium (CVSS: 6.5)
NVT: Joomla! < 3.8.13 ACL Violation Vulnerability

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary
If an attacker gets access to the mail account of an user who can approve admin verifications in the registration process, he can activate himself.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.8.13
Installation
path / port:       /joomla
```

Solution
Solution type: VendorFix
Update to version 3.8.13 or later.

Affected Software/OS
Joomla! CMS versions 1.5.0 through 3.8.12.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! < 3.8.13 ACL Violation Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141580

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2018-17855
url: https://developer.joomla.org/security-centre/754-20181004-core-acl-violatio
↪n-in-com-users-for-the-admin-verification
dfn-cert: DFN-CERT-2018-2061
```

Medium (CVSS: 5.8)
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.

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

References

```
cve: CVE-2014-0224
bid: 67899
url: https://www.openssl.org/news/secadv/20140605.txt
url: http://www.securityfocus.com/bid/67899
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0384
cert-bund: CB-K15/0080
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

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.

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

References

```
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
bid: 9506
bid: 9561
bid: 11604
bid: 15222
bid: 19915
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
bid: 24456
bid: 33374
bid: 36956
bid: 36990
bid: 37995
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
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

Medium (CVSS: 5.0)
NVT: MacOS X Finder '.DS_Store' Information Disclosure

Summary
MacOS X creates a hidden file '.DS_Store', in each directory that has been viewed with the 'Finder'. This file contains a list of the contents of the directory, giving an attacker information on the structure and contents of your website.

Vulnerability Detection Result

```
The following files were identified:
https://owasp/cyclone/.DS_Store
https://owasp/cyclone/uploads/.DS_Store
```

Solution
Solution type: Workaround
Block access to hidden files (starting with a dot) within your webservers configuration

Vulnerability Detection Method
Details: `MacOS X Finder '.DS_Store' Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.10756

References

```
cve: CVE-2016-1776
cve: CVE-2018-6470
bid: 3316
bid: 3324
bid: 85054
url: https://www.securityfocus.com/bid/3316
url: https://www.securityfocus.com/bid/3324
url: https://www.securityfocus.com/bid/85054
url: https://helpx.adobe.com/dreamweaver/kb/remove-ds-store-files-mac.html
url: https://support.apple.com/en-us/HT1629
cert-bund: CB-K16/0450
dfn-cert: DFN-CERT-2016-0489
```

Medium (CVSS: 5.0)
NVT: Joomla! Core LDAP Information Disclosure Vulnerability Nov17

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.8.2
```

Impact

Successfully exploiting this issue allow remote attackers to disclose username and password.

Solution

Solution type: VendorFix
Upgrade to Joomla version 3.8.2 or later.

Affected Software/OS

Joomla core version 1.5.0 through 3.8.1

Vulnerability Insight

The flaw exists due to an inadequate escaping in the LDAP authentication plugin.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Joomla! Core LDAP Information Disclosure Vulnerability Nov17`
OID:1.3.6.1.4.1.25623.1.0.811896

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2017-14596
bid: 100898
url: https://developer.joomla.org/security-centre/714-20171101-core-ldap-informa
↪tion-disclosure.html
url: https://blog.ripstech.com/2017/joomla-takeover-in-20-seconds-with-ldap-inje
↪ction-cve-2017-14596
cert-bund: CB-K17/1899
cert-bund: CB-K17/1591
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1977
dfn-cert: DFN-CERT-2017-1663
```

Medium (CVSS: 5.0)
NVT: Source Control Management (SCM) Files Accessible

Summary
The script attempts to identify files of a SCM accessible at the webserver.

Vulnerability Detection Result

```
The following SCM files/folders were identified:
https://owasp/zapwave/.svn/wc.db
https://owasp/mutillidae/.git/logs/HEAD
https://owasp/mutillidae/.git/config
https://owasp/mutillidae/.git/description
https://owasp/mutillidae/.git/FETCH_HEAD
https://owasp/mutillidae/.git/ORIG_HEAD
https://owasp/mutillidae/.git/HEAD
https://owasp/MCIR/.git/logs/HEAD
https://owasp/MCIR/.git/config
https://owasp/MCIR/.git/description
https://owasp/MCIR/.git/FETCH_HEAD
https://owasp/MCIR/.git/ORIG_HEAD
https://owasp/MCIR/.git/HEAD
https://owasp/dvwa/.git/logs/HEAD
https://owasp/dvwa/.git/config
https://owasp/dvwa/.git/description
https://owasp/dvwa/.git/FETCH_HEAD
https://owasp/dvwa/.git/ORIG_HEAD
https://owasp/dvwa/.git/HEAD
```

Impact
Based on the information provided in this files an attacker might be able to gather additional info about the structure of the system and its applications.

Solution
Solution type: Mitigation
Restrict access to the Admin Pages for authorized systems only.

Vulnerability Insight
Currently the script is checking for files of the following SCM:
- Git (.git)
- Mercurial (.hg)
- Bazaar (.bzr)
- CVS (CVS/Root, CVS/Entries)
- Subversion (.svn)

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Check the response if SCM files are accessible.
Details: `Source Control Management (SCM) Files Accessible`
OID:1.3.6.1.4.1.25623.1.0.111084

References

```
url: http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-be
↪long-to-us
url: https://github.com/anantshri/svn-extractor
url: https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d
url: https://blog.netspi.com/dumping-git-data-from-misconfigured-web-servers/
url: http://resources.infosecinstitute.com/hacking-svn-git-and-mercurial/
```

Medium (CVSS: 5.0)
NVT: Joomla! < 3.8.0 LDAP Information Disclosure Vulnerability

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.8.0
```

Impact

Successfully exploiting these issues will allow remote attackers to gain access to potentially sensitive information.

Solution

Solution type: VendorFix
Upgrade to Joomla version 3.8.0 or later.

Affected Software/OS

Joomla! versions 1.5.0 through 3.7.5

Vulnerability Insight

Joomla is prone to the following information disclosure vulnerability:
- Inadequate escaping in the LDAP authentication plugin can result into a disclosure of username and password.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Joomla! < 3.8.0 LDAP Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112049

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2017-14596
url: https://developer.joomla.org/security-centre/711-20170902-core-ldap-informa
↪tion-disclosure
cert-bund: CB-K17/1899
cert-bund: CB-K17/1591
dfn-cert: DFN-CERT-2017-1977
dfn-cert: DFN-CERT-2017-1663
```

Medium (CVSS: 5.0)
NVT: Joomla! Information Disclosure and Cross-Site Scripting Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary
This host is running Joomla and is prone to information disclosure and cross-site scripting vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.7.0
```

Impact
Successfully exploiting these issues allow remote attackers to gain access to potentially sensitive information and conduct cross-site scripting attacks.

Solution
Solution type: VendorFix
Upgrade to Joomla version 3.7.0 or later.

Affected Software/OS
Joomla core versions 1.5.0 through 3.6.5

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Multiple flaws are due to,
- Mail sent using the JMail API leaked the used PHPMailer version in the mail headers.
- Inadequate filtering of specific HTML attributes.
- Inadequate filtering of multibyte characters.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Joomla! Information Disclosure and Cross-Site Scripting Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.811042

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2017-7983
cve: CVE-2017-7986
cve: CVE-2017-7985
bid: 98016
bid: 98024
bid: 98020
url: https://developer.joomla.org/security-centre/686-20170404-core-xss-vulnerab
↪ility
url: https://developer.joomla.org/security-centre/685-20170403-core-xss-vulnerab
↪ility
url: https://developer.joomla.org/security-centre/683-20170401-core-information-
↪disclosure
cert-bund: CB-K17/1113
cert-bund: CB-K17/0698
dfn-cert: DFN-CERT-2017-1151
dfn-cert: DFN-CERT-2017-0720
```

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware ’fixedURLData’ Local File Inclusion Vulnerability

Product detection result

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

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
url: http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-r
↪eleased
url: https://sourceforge.net/p/tikiwiki/code/60308/
url: https://tiki.org
```

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)
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

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: CVE-2008-5319
url: http://secunia.com/advisories/32341
url: http://info.tikiwiki.org/tiki-read_article.php?articleId=41
```

Medium (CVSS: 5.0)
NVT: Sensitive File Disclosure (HTTP)

Summary
The script attempts to identify files containing sensitive data at the remote web server like e.g.:
- software (Blog, CMS) configuration

. . . continues on next page . . .

. . . continued from previous page . . .

- database backup files
- SSH or SSL/TLS Private-Keys

Vulnerability Detection Result

```
The following files containing sensitive information were identified (URL:Descri
↪ption):
https://owasp/redmine/config/database.yml:Rails Database Configuration File cont
↪aining a username and/or password.
```

Impact

Based on the information provided in this files an attacker might be able to gather additional info and/or sensitive data like usernames and passwords.

Solution

Solution type: Mitigation

The sensitive files shouldn't be accessible via a web server. Restrict access to it or remove it completely.

Vulnerability Detection Method

Enumerate the remote web server and check if sensitive files are accessible.

Details: `Sensitive File Disclosure (HTTP)`

OID:1.3.6.1.4.1.25623.1.0.107305

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result

```
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

Affected Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method

Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031

References

```
cve: CVE-2016-2183
cve: CVE-2016-6329
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
```

. . . continues on next page . . .

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

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

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

Vulnerability Detection Result

```
Vulnerable URL: https://owasp/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.

Affected Software/OS
awiki 20100125 is vulnerable. Other versions may also be affected.

Vulnerability Detection Method
Details: `awiki Multiple Local File Include Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.103210

References

```
bid: 49187
url: https://www.exploit-db.com/exploits/36047/
url: http://www.securityfocus.com/bid/49187
```

... continues on next page ...

... continued from previous page ...

```
url: http://www.kobaonline.com/awiki/
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary

Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
path / port:       /
```

Solution

Solution type: VendorFix

Update to version 1.6.3 or later or apply the patch.

Affected Software/OS

jQuery prior to version 1.6.3.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `jQuery < 1.6.3 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141637

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.7.2`

Method: `jQuery Detection (HTTP)`

OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

```
Installed version: 1.8.2
Fixed version:     1.9.0
Installation
path / port:       /owaspbricks/javascripts
```

Solution

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `jQuery < 1.9.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141636

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.7.2`

Method: `jQuery Detection (HTTP)`

OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /mutillidae/javascript/ddsmoothmenu
```

Solution

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 4.3)
NVT: Joomla! Core 'Media Manager' XSS Vulnerability (20180509)

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to a cross site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.8.8
Installation
path / port:       /joomla
```

Impact

Successful exploitation will allow remote attackers to conduct XSS attack.

Solution

Solution type: VendorFix

Upgrade to Joomla version 3.8.8 or later. Please see the references for more information.

Affected Software/OS

Joomla core versions 1.5.0 through 3.8.7

Vulnerability Insight

The flaw exists due to inadequate filtering of file and folder names in media manager.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Joomla! Core 'Media Manager' XSS Vulnerability (20180509)`

OID:1.3.6.1.4.1.25623.1.0.813406

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`

Method: `joomla Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2018-6378
url: https://developer.joomla.org/security-centre/737-20180509-core-xss-vulnerab
↪ility-in-the-media-manager.html
dfn-cert: DFN-CERT-2018-0979
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /
```

Solution

Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.7.2
Detected by jQuery Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.141622)
```

Summary

Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
path / port:       /mutillidae/javascript/ddsmoothmenu
```

Solution

Solution type: VendorFix

Update to version 1.6.3 or later or apply the patch.

Affected Software/OS

jQuery prior to version 1.6.3.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.7.2`
Method: `jQuery Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.141622)

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

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

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:phpmyadmin:phpmyadmin:3.3.2 -
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.

Affected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

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

Vulnerability Detection Method
Details: `phpMyAdmin 'error.php' Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801660

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.3.2 -`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References

```
cve: CVE-2010-4480
url: http://www.exploit-db.com/exploits/15699/
url: http://www.vupen.com/english/advisories/2010/3133
dfn-cert: DFN-CERT-2011-0467
dfn-cert: DFN-CERT-2011-0451
dfn-cert: DFN-CERT-2011-0016
dfn-cert: DFN-CERT-2011-0002
```

Medium (CVSS: 4.3)
NVT: Tiki Wiki < 21.2 XSS 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

Tiki Wiki is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     21.2
Installation
path / port:       /tikiwiki
```

Impact

Successful exploitation would allow an attacker to inject arbitrary HTML and JavaScript into the site.

Solution

Solution type: VendorFix

Update to version 21.2.

Affected Software/OS

Tiki Wiki through version 21.1.

Vulnerability Insight

The vulnerability exists because some patterns are not properly considered in lib/core/TikiFilter/PreventXss.php.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Tiki Wiki < 21.2 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.113737

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-2020-16131
url: https://gitlab.com/tikiwiki/tiki/-/commit/d12d6ea7b025d3b3f81c8a71063fe9f89
↪e0c4bf1
```

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

References

```
cve: CVE-2014-3566
bid: 70574
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-exploitin
↪g-ssl-30.html
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1102
cert-bund: CB-K16/0599
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
```

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

Medium (CVSS: 4.3)
NVT: OrangeHRM 'jobVacancy.php' Cross Site Scripting Vulnerability

Product detection result

```
cpe:/a:orangehrm:orangehrm:2.4.2
Detected by OrangeHRM Detection (OID: 1.3.6.1.4.1.25623.1.0.100850)
```

Summary

OrangeHRM is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input before using it in dynamically generated content.

Vulnerability Detection Result

```
Vulnerable URL: https://owasp/orangehrm/templates/recruitment/jobVacancy.php?rec
↪ruitcode=</script><script>alert('vt-xss-test')</script>
```

Impact

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other 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.

Affected Software/OS

... continues on next page ...

. . . continued from previous page . . .

OrangeHRM 2.6.2 is vulnerable. Other versions may also be affected.

Vulnerability Detection Method
Details: `OrangeHRM 'jobVacancy.php' Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103132

Product Detection Result
Product: `cpe:/a:orangehrm:orangehrm:2.4.2`
Method: `OrangeHRM Detection`
OID: 1.3.6.1.4.1.25623.1.0.100850)

References
```
bid: 47046
url: https://www.securityfocus.com/bid/47046
```

Medium (CVSS: 4.3)
NVT: Joomla! 'Uri' class XSS Vulnerability

Product detection result
```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary
This host is running Joomla and is prone to cross site scripting vulnerability.

Vulnerability Detection Result
```
Installed version: 1.5.15
Fixed version:     3.8.4
Installation
path / port:       /joomla
```

Impact
Successfully exploiting this issue will allow remote attackers to execute arbitrary javascript code in the context of current user.

Solution
Solution type: VendorFix
Upgrade to Joomla version 3.8.4 or later.

Affected Software/OS
Joomla core version 1.5.0 through 3.8.3

Vulnerability Insight
The flaw exists due to inadequate input filtering in the Uri class (formerly JUri).

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Joomla! 'Uri' class XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.812681

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2018-6379
url: https://developer.joomla.org/security-centre/721-20180104-core-xss-vulnerab
↪ility.html
cert-bund: CB-K18/0197
dfn-cert: DFN-CERT-2018-0214
```

Medium (CVSS: 4.3)
NVT: Tiki Wiki CMS Groupware < 21.0 XSS 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

Tiki Wiki is prone to a cross-site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     21.0
Installation
path / port:       /tikiwiki
```

Solution

Solution type: VendorFix
Update to version 21.0.

Affected Software/OS

Tiki Wiki CMS Groupware version 20.0 and prior.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Some php pages receive input from an upstream component, but do not neutralize or incorrectly neutralize special characters such as '<', '>', and '&'. These characters could be interpreted as web-scripting elements when they are sent to a downstream component that processes web pages.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki CMS Groupware < 21.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112721

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-2020-8966
url: https://www.incibe-cert.es/en/early-warning/security-advisories/cross-site-
↪scripting-xss-flaws-found-tiki-wiki-cms-software
```

Medium (CVSS: 4.3)
NVT: Joomla! Multiple Cross-site Scripting Vulnerabilities

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary
This host is running Joomla and is prone to multiple Cross-site scripting vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     1.5.21
```

Impact
Successful exploitation will allow attackers to inject arbitrary web script or HTML via vectors involving 'multiple encoded entities'.

Solution
Solution type: VendorFix
Upgrade to Joomla! 1.5.21 or later.

Affected Software/OS
Joomla! versions 1.5.x before 1.5.21

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The flaws are due to inadequate filtering of multiple encoded entities, which could be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser in the security context of an affected Web site.

Vulnerability Detection Method

Details: `Joomla! Multiple Cross-site Scripting Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.901168

Product Detection Result

Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2010-3712
url: http://www.vupen.com/english/advisories/2010/2615
url: http://developer.joomla.org/security/news/9-security/10-core-security/322-2
↪0101001-core-xss-vulnerabilities
```

Medium (CVSS: 4.3)
NVT: Joomla! Core Cross-Site Scripting Vulnerability - July17

Product detection result

```
cpe:/a:joomla:joomla:1.5.15
Detected by joomla Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100330)
```

Summary

This host is running Joomla and is prone to cross-site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.7.4
```

Impact

Successfully exploiting this issue will allow remote attacker to conduct cross-site scripting attacks.

Solution

Solution type: VendorFix
Upgrade to Joomla version 3.7.4 or later.

Affected Software/OS

Joomla core versions 1.5.0 through 3.7.3

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight
The flaw exists due to Inadequate filtering of potentially malicious HTML tags in various components of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! Core Cross-Site Scripting Vulnerability - July17`
OID:1.3.6.1.4.1.25623.1.0.811257

Product Detection Result
Product: `cpe:/a:joomla:joomla:1.5.15`
Method: `joomla Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100330)

References

```
cve: CVE-2017-11612
url: https://developer.joomla.org/security-centre/701-20170704-core-installer-la
↪ck-of-ownership-verification
cert-bund: CB-K17/1245
dfn-cert: DFN-CERT-2017-1286
```

Medium (CVSS: 4.3)
NVT: Apache Web Server ETag Header Information Disclosure Weakness

Product detection result

```
cpe:/a:apache:http_server:2.2.14
Detected by Apache HTTP/Web Server Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.
↪900498)
```

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: 286483
Size: 28067
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

Product Detection Result

Product: `cpe:/a:apache:http_server:2.2.14`
Method: `Apache HTTP/Web Server Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900498)

References

```
cve: CVE-2003-1418
bid: 6939
url: https://www.securityfocus.com/bid/6939
url: http://httpd.apache.org/docs/mod/core.html#fileetag
url: http://www.openbsd.org/errata32.html
url: http://support.novell.com/docs/Tids/Solutions/10090670.html
cert-bund: CB-K17/1750
cert-bund: CB-K17/0896
cert-bund: CB-K15/0469
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-0925
dfn-cert: DFN-CERT-2015-0495
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

References

```
cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverab
↪les/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
cert-bund: CB-K18/0094
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
cert-bund: CB-K16/1384
cert-bund: CB-K16/1141
cert-bund: CB-K16/1107
cert-bund: CB-K16/1102
cert-bund: CB-K16/0792
cert-bund: CB-K16/0599
cert-bund: CB-K16/0597
cert-bund: CB-K16/0459
cert-bund: CB-K16/0456
cert-bund: CB-K16/0433
cert-bund: CB-K16/0424
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/0415
cert-bund: CB-K16/0413
cert-bund: CB-K16/0374
cert-bund: CB-K16/0367
cert-bund: CB-K16/0331
cert-bund: CB-K16/0329
cert-bund: CB-K16/0328
cert-bund: CB-K16/0156
cert-bund: CB-K15/1514
cert-bund: CB-K15/1358
cert-bund: CB-K15/1021
cert-bund: CB-K15/0972
cert-bund: CB-K15/0637
cert-bund: CB-K15/0590
cert-bund: CB-K15/0525
cert-bund: CB-K15/0393
cert-bund: CB-K15/0384
cert-bund: CB-K15/0287
cert-bund: CB-K15/0252
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K15/0118
cert-bund: CB-K15/0110
cert-bund: CB-K15/0108
cert-bund: CB-K15/0080
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
cert-bund: CB-K15/0075
cert-bund: CB-K14/1617
cert-bund: CB-K14/1581
cert-bund: CB-K14/1537
cert-bund: CB-K14/1479
cert-bund: CB-K14/1458
cert-bund: CB-K14/1342
cert-bund: CB-K14/1314
cert-bund: CB-K14/1313
cert-bund: CB-K14/1311
cert-bund: CB-K14/1304
cert-bund: CB-K14/1296
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2016-1929
dfn-cert: DFN-CERT-2016-1527
dfn-cert: DFN-CERT-2016-1468
dfn-cert: DFN-CERT-2016-1216
dfn-cert: DFN-CERT-2016-1174
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0884
dfn-cert: DFN-CERT-2016-0841
dfn-cert: DFN-CERT-2016-0644
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0495
dfn-cert: DFN-CERT-2016-0465
dfn-cert: DFN-CERT-2016-0459
dfn-cert: DFN-CERT-2016-0453
dfn-cert: DFN-CERT-2016-0451
dfn-cert: DFN-CERT-2016-0415
dfn-cert: DFN-CERT-2016-0403
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2016-0360
dfn-cert: DFN-CERT-2016-0359
dfn-cert: DFN-CERT-2016-0357
dfn-cert: DFN-CERT-2016-0171
dfn-cert: DFN-CERT-2015-1431
dfn-cert: DFN-CERT-2015-1075
dfn-cert: DFN-CERT-2015-1026
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2015-0548
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0118
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0083
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
dfn-cert: DFN-CERT-2014-1717
dfn-cert: DFN-CERT-2014-1680
dfn-cert: DFN-CERT-2014-1632
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1542
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-1366
dfn-cert: DFN-CERT-2014-1354
```

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
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

References

```
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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

References

```
cve: CVE-2012-0053
bid: 51706
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.html
cert-bund: CB-K15/0080
cert-bund: CB-K14/1505
cert-bund: CB-K14/0608
dfn-cert: DFN-CERT-2015-0082
dfn-cert: DFN-CERT-2014-1592
dfn-cert: DFN-CERT-2014-0635
dfn-cert: DFN-CERT-2013-1307
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1112
dfn-cert: DFN-CERT-2012-0928
dfn-cert: DFN-CERT-2012-0758
dfn-cert: DFN-CERT-2012-0744
dfn-cert: DFN-CERT-2012-0568
dfn-cert: DFN-CERT-2012-0425
dfn-cert: DFN-CERT-2012-0424
dfn-cert: DFN-CERT-2012-0387
dfn-cert: DFN-CERT-2012-0343
dfn-cert: DFN-CERT-2012-0332
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0306
dfn-cert: DFN-CERT-2012-0264
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188
```

Medium (CVSS: 4.3)
NVT: Tiki Wiki CMS Groupware Multiple Cross Site Scripting Vulnerabilities

Product detection result

```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary

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

Vulnerability Detection Result

```
Vulnerable URL: https://owasp/tikiwiki/tiki-listpages.php/<script>alert("XSS_Che
↪ck");</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

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)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2009-1204
bid: 34105
bid: 34106
bid: 34107
bid: 34108
url: http://secunia.com/advisories/34273
url: http://info.tikiwiki.org/tiki-read_article.php?articleId=51
```

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

Summary

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

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              CN=owaspbwa
Signature Algorithm:  sha1WithRSAEncryption
```

Solution

Solution type: Mitigation

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

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

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

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

Fingerprint1

or

fingerprint1,Fingerprint2

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880

References
`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: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

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

Vulnerability Detection Result

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

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

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see 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

References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

[return to 10.0.2.4]

2.1.10 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
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/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

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
url: http://openwall.com/lists/oss-security/2018/02/16/1
```

Low (CVSS: 3.5)
NVT: Tiki Wiki CMS Groupware 18.4 XSS 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
Tiki Wiki is prone to a cross-site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     None
Installation
path / port:       /tikiwiki
```

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.

Affected Software/OS
Tiki Wiki CMS Groupware version 18.4 and probably prior.

Vulnerability Insight
tiki/tiki-upload_file.php allows remote attackers to upload JavaScript code that is executed upon visiting a tiki/tiki-download_file.php?display&fileId= URI.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki CMS Groupware 18.4 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.142795

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-2019-15314
url: https://pastebin.com/wEM7rnG7
```

Low (CVSS: 2.6)
NVT: Apache mod_perl 'Apache::Status' and 'Apache2::Status' Cross Site Scripting Vulnerability

Summary
According to its version number, the remote version of the Apache mod_perl module is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 2.0.4
Fixed version:     See references
```

Impact

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

Solution

Solution type: VendorFix

The vendor has released a fix through the SVN repository.

Vulnerability Detection Method

Details: `Apache mod_perl 'Apache::Status' and 'Apache2::Status' Cross Site Scripting Vul.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.100130

References

```
cve: CVE-2009-0796
bid: 34383
url: http://www.securityfocus.com/bid/34383
url: http://mail-archives.apache.org/mod_mbox/perl-advocacy/200904.mbox/<ad28918
↪e0904011458h273a71d4x408f1ed286c9dfbc@mail.gmail.com>
dfn-cert: DFN-CERT-2009-1816
dfn-cert: DFN-CERT-2009-1576
dfn-cert: DFN-CERT-2009-0490
```

[return to 10.0.2.4]

2.1.11 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

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

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 19688635
Packet 2: 19688907
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

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

Solution

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091

References

```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 10.0.2.4]

2.1.12 Low 22/tcp

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

Summary

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

Vulnerability Detection Result

```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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

[return to 10.0.2.4]

2.1.13 Low 443/tcp

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

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Tiki Wiki CMS Groupware XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.140797

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
url: http://openwall.com/lists/oss-security/2018/02/16/1
```

Low (CVSS: 3.5)
NVT: Tiki Wiki CMS Groupware 18.4 XSS 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
Tiki Wiki is prone to a cross-site scripting vulnerability.

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     None
Installation
path / port:       /tikiwiki
```

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.

Affected Software/OS
Tiki Wiki CMS Groupware version 18.4 and probably prior.

Vulnerability Insight
tiki/tiki-upload_file.php allows remote attackers to upload JavaScript code that is executed upon visiting a tiki/tiki-download_file.php?display&fileId= URI.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki CMS Groupware 18.4 XSS Vulnerability`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.142795

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-2019-15314
url: https://pastebin.com/wEM7rnG7
```

Low (CVSS: 2.6)
NVT: SSL/TLS: TLS/SPDY Protocol Information Disclosure Vulnerability (CRIME)

Summary

The TLS/SPDY protocols are prone to an information-disclosure vulnerability.

Vulnerability Detection Result

```
The remote service might be vulnerable to the "CRIME" attack because it provides
↪ the following TLS compression methods:
Protocol:Compression Method
TLSv1.0:DEFLATE
SSLv3:DEFLATE
```

Impact

A man-in-the-middle attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

Solution

Solution type: Mitigation

Disable TLS compression in the configuration of this services. If SPDY below 4 is used upgrade the webserver to a version which supports the successor protocol SPDY/4 or HTTP/2.
Please see the references for more resources supporting you with this task.

Affected Software/OS

Services enabling TLS compression or supporting the SPDY protocol below SPDY/4 via HTTPS.

Vulnerability Detection Method

Details: `SSL/TLS: TLS/SPDY Protocol Information Disclosure Vulnerability (CRIME)`
OID:1.3.6.1.4.1.25623.1.0.108094

References

```
cve: CVE-2012-4929
cve: CVE-2012-4930
bid: 55704
bid: 55707
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/55704
url: http://www.securityfocus.com/bid/55707
url: http://permalink.gmane.org/gmane.comp.lib.qt.devel/6729
url: https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2012/septem
↪ber/details-on-the-crime-attack/
cert-bund: CB-K17/0504
cert-bund: CB-K15/0637
cert-bund: CB-K14/1342
cert-bund: CB-K14/0458
cert-bund: CB-K13/0882
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2014-0483
dfn-cert: DFN-CERT-2013-1893
dfn-cert: DFN-CERT-2013-0672
dfn-cert: DFN-CERT-2013-0631
dfn-cert: DFN-CERT-2013-0469
dfn-cert: DFN-CERT-2013-0324
dfn-cert: DFN-CERT-2013-0321
dfn-cert: DFN-CERT-2013-0112
dfn-cert: DFN-CERT-2012-2191
dfn-cert: DFN-CERT-2012-2062
dfn-cert: DFN-CERT-2012-1973
dfn-cert: DFN-CERT-2012-1966
```

Low (CVSS: 2.6)
NVT: Apache mod_perl 'Apache::Status' and 'Apache2::Status' Cross Site Scripting Vulnerability

Summary
According to its version number, the remote version of the Apache mod_perl module is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.

Vulnerability Detection Result

```
Installed version: 2.0.4
Fixed version:     See references
```

Impact
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

Solution
Solution type: VendorFix
The vendor has released a fix through the SVN repository.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `Apache mod_perl 'Apache::Status' and 'Apache2::Status' Cross Site Scripting Vul.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.100130

References

```
cve: CVE-2009-0796
bid: 34383
url: http://www.securityfocus.com/bid/34383
url: http://mail-archives.apache.org/mod_mbox/perl-advocacy/200904.mbox/<ad28918
↪e0904011458h273a71d4x408f1ed286c9dfbc@mail.gmail.com>
dfn-cert: DFN-CERT-2009-1816
dfn-cert: DFN-CERT-2009-1576
dfn-cert: DFN-CERT-2009-0490
```

[return to 10.0.2.4]