Scan Report

November 2, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP 172.20.10.3”. The scan started at Sat Nov 2 11:45:44 2024 UTC and ended at . 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
172.20.10.3	38	75	5	0	0
Total: 1	38	75	5	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 118 results selected by the filtering described above. Before filtering there were 1108 results.

2 Results per Host

2.1 172.20.10.3

Host scan start	Sat Nov 2 11:47:33 2024 UTC
Host scan end	

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

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

Summary
The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection (QoD): 80%

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
```

Impact
An EOL version of an OS 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: Mitigation
Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method
Checks if an EOL version of an OS is present on the target host.
Details: `Operating System (OS) End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: `2024-02-28T14:37:42Z`

[return to 172.20.10.3]

2.1.2 High 8080/tcp

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

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

Quality of Detection (QoD): 98%

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
It was possible to login into the Tomcat Host Manager at http://172.20.10.3:8080
↪/host-manager/html using user "root" with password "owaspbwa"
It was possible to login into the Tomcat Manager at http://172.20.10.3:8080/mana
↪ger/html using user "root" with password "owaspbwa"
It was possible to login into the Tomcat Server Status at http://172.20.10.3:808
↪0/manager/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

Version used: `2023-07-25T05:05:58Z`

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
url: https://www.zerodayinitiative.com/advisories/ZDI-10-214/
url: http://www.securityfocus.com/bid/36258
url: http://www.securityfocus.com/bid/36954
url: http://www.securityfocus.com/bid/37086
url: http://www.securityfocus.com/bid/38084
url: http://www.securityfocus.com/bid/44172
url: http://www.securityfocus.com/bid/79264
url: http://www.securityfocus.com/bid/79351
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 172.20.10.3]

2.1.3 High 443/tcp

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

Summary
The Tiki Wiki CMS Groupware version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Quality of Detection (QoD): 80%

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 EOL 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 an EOL version is present on the target host.
Details: `Tiki Wiki CMS Groupware End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.108622
Version used: `2023-09-19T05:06:03Z`

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

High (CVSS: 9.8)
NVT: Joomla! < 3.8.0 LDAP Information Disclosure Vulnerability

Summary
Joomla is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

. . . continues on next page . . .

. . . continued from previous page . . .

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

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

Version used: `2023-07-14T16:09:27Z`

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
```

High (CVSS: 9.8)

NVT: Joomla! Core LDAP Information Disclosure Vulnerability (Nov 2017)

Summary

Joomla is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
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 (Nov 2017)`

OID:1.3.6.1.4.1.25623.1.0.811896

Version used: `2024-02-20T05:05:48Z`

References

```
cve: CVE-2017-14596
url: https://developer.joomla.org/security-centre/714-20171101-core-ldap-informa
↪tion-disclosure.html
url: http://www.securityfocus.com/bid/100898
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
```

High (CVSS: 9.8)

NVT: Joomla < 3.9.5 Multiple Vulnerabilities

Summary

Joomla! is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.9.5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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

Version used: `2021-09-02T13:01:30Z`

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: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-0239
cert-bund: WID-SEC-2022-1948
cert-bund: WID-SEC-2022-1947
cert-bund: WID-SEC-2022-0732
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K21/1083
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-K19/0329
cert-bund: CB-K19/0287
dfn-cert: DFN-CERT-2023-2027
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-0481
dfn-cert: DFN-CERT-2023-0245
dfn-cert: DFN-CERT-2022-2467
dfn-cert: DFN-CERT-2021-1536
dfn-cert: DFN-CERT-2021-1503
dfn-cert: DFN-CERT-2021-0826
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: 9.8)
NVT: Joomla < 3.8.12 Multiple Vulnerabilities

Summary
Joomla is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

Solution:
Solution type: VendorFix
Update 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
Version used: `2021-09-29T12:07:39Z`

. . . continues on next page . . .

. . . continued from previous page . . .

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
```

High (CVSS: 9.8)
NVT: Joomla! < 3.9.7 Multiple Vulnerabilities

Summary

Joomla! is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

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.

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

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2023-01-31T10:08:41Z

References

```
cve: CVE-2019-12764
cve: CVE-2019-12765
cve: CVE-2019-12766
url: https://developer.joomla.org/security-centre/785-20190603-core-acl-hardenin
↪g-of-com-joomlaupdate
url: http://www.securityfocus.com/bid/108729
url: http://www.securityfocus.com/bid/108735
url: http://www.securityfocus.com/bid/108736
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: 8.8)
NVT: Tiki Wiki < 22 Multiple Vulnerabilities

Summary

Tiki Wiki is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     22
Installation
path / port:       /tikiwiki
```

Impact

- Local (php) File Inclusion: The config file displays TikiWikis database credentials in cleartext.
- Cross-Site Request Forgery (CSRF): A successful exploit could allow the attacker to perform arbitrary actions on an affected system with the privileges of the user. These action include allowing attackers to submit their own code through an authenticated user resulting in local file Inclusion. If an authenticated user who is able to edit Tiki Wiki templates visits an malicious website, template code can be edited.
- Information Exposure: The User can authenticate against it and simply give itself admin privileges or compromise the administrator account.

Solution:

Solution type: VendorFix

Update to version 22 which disables and hides the risky preferences by default.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Tiki Wiki through version 21.2 and probably prior.

Vulnerability Insight

The following flaws exist:

- Local (php) File Inclusion: In TikiWiki, an user can be given the permission to edit .tpl templates. This feature can be abused to escalate the users privileges by inserting the following pieceof smarty code: }include file='../db/local.php'}. The code snippet includes Tiki Wikis database configuration file and displays it in the pages source code. Any other www-data readable file like '/etc/passwd' can be included as well.

- Cross-Site Request Forgery (CSRF): Tiki Wiki allows templates to be edited without CSRF protection. This could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to follow a maliciously crafted link. (CVE-2020-29254)

- Information Exposure: An user who is able to edit template files can use smarty code to include Files like the database configuration file which allows access to TikiWikis Database.

Vulnerability Detection Method

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

Details: `Tiki Wiki < 22 Multiple Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.144911

Version used: `2024-06-28T05:05:33Z`

References

```
cve: CVE-2020-29254
url: https://doc.tiki.org/CVE-2020-29254
url: https://github.com/S1lkys/CVE-2020-29254
url: https://github.com/S1lkys/CVE-2020-29254/blob/main/Tiki-Wiki%2021.2%20by%20
↪Maximilian%20Barz.pdf
```

High (CVSS: 8.8)
NVT: OrangeHRM <= 4.3.1 RCE Vulnerability

Summary

OrangeHRM is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 2.4.2
Fixed version:     4.3.2
Installation
path / port:       /orangehrm
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation would allow an authenticated attacker to execute arbitrary code on the target machine.

Solution:
Solution type: VendorFix
Update to version 4.3.2 or later.

Affected Software/OS
OrangeHRM through version 4.3.1.

Vulnerability Insight
The vulnerability exists due to an input validation error within admin/listMailConfiguration (txtSendmailPath parameter).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OrangeHRM <= 4.3.1 RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113416
Version used: `2024-05-30T05:05:32Z`

References

```
cve: CVE-2019-12839
url: https://github.com/orangehrm/orangehrm/releases/tag/4.3.2
url: https://ctrsec.io/research/2019/06/12/ace-orangehrm.html
url: https://github.com/orangehrm/orangehrm/pull/528
```

High (CVSS: 8.8)
NVT: Tiki Wiki < 24.1 Multiple Vulnerabilities

Summary
Tiki Wiki is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     24.1
Installation
path / port:       /tikiwiki
```

Solution:
Solution type: VendorFix
Update to version 24.1.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Tiki Wiki prior to version 24.1.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2023-22850: PHP object injection in /lib/sheet/grid.php
- CVE-2023-22853: PHP code injection in /lib/structures/structlib.php

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki < 24.1 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.127300
Version used: `2023-10-13T05:06:10Z`

References
```
cve: CVE-2023-22850
cve: CVE-2023-22853
url: https://karmainsecurity.com/KIS-2023-03
url: https://karmainsecurity.com/KIS-2023-02
```

High (CVSS: 8.8)
NVT: Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability

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

Quality of Detection (QoD): 80%

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`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.141885
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2018-20719
url: https://blog.ripstech.com/2018/scan-verify-patch-security-issues-in-minutes
↪/
```

High (CVSS: 8.8)
NVT: Joomla! < 3.8.13 ACL Violation Vulnerability

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.

Quality of Detection (QoD): 80%

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
Version used: `2023-07-20T05:05:17Z`

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
```

High (CVSS: 8.8)
NVT: Joomla! < 3.9.13 Multiple Vulnerabilities

Summary
Joomla! is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

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
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
Version used: `2021-09-02T13:01:30Z`

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
```

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

Summary
Joomla! is prone to multiple security vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.5.15
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
Joomla! versions prior to 1.6.1.

Vulnerability Insight
The following flaws exist:
- 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 Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! < 1.6.1 Multiple Security Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.103114
Version used: `2022-07-22T10:11:18Z`

References

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

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

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

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

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

Vulnerability Detection Method
Details: `Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100537
Version used: `2024-03-01T14:37:10Z`

References

```
cve: CVE-2010-1135
cve: CVE-2010-1134
cve: CVE-2010-1133
cve: CVE-2010-1136
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: 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.

Quality of Detection (QoD): 98%

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.

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
Version used: `2024-06-14T05:05:48Z`

References

```
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K21/1094
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

High (CVSS: 7.5)
NVT: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability

Summary
Tiki Wiki CMS Groupware is prone to a local file inclusion vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

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

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

Affected Software/OS
Tiki Wiki CMS Groupware versions:
- below 12.11 LTS
- 13.x, 14.x and 15.x below 15.4

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.108064
Version used: `2024-03-01T14:37:10Z`

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/
```

High (CVSS: 7.5)
NVT: HTTP Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote Web Application using default credentials.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

```
It was possible to login with the following credentials (<URL>:<User>:<Password>
↪:<HTTP status code>)
https://172.20.10.3/WebGoat/attack:user:user:HTTP/1.1 200 OK
```

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

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

Vulnerability Insight
As the VT 'HTTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports default credentials detected by the VT 'HTTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041).
Details: `HTTP Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103240
Version used: `2022-08-04T13:37:02Z`

References

```
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
```

High (CVSS: 7.4)
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Summary
OpenSSL is prone to security-bypass vulnerability.

Quality of Detection (QoD): 70%

... continues on next page ...

. . . continued from previous page . . .

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

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

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

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

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

Vulnerability Detection Method
Send two SSL ChangeCipherSpec request and check the response.
Details: `SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105042
Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-0224
url: https://www.openssl.org/news/secadv/20140605.txt
url: http://www.securityfocus.com/bid/67899
cert-bund: WID-SEC-2023-0500
cert-bund: CB-K15/0567
cert-bund: CB-K15/0415
cert-bund: CB-K15/0384
cert-bund: CB-K15/0080
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
```

High (CVSS: 7.2)
NVT: Tiki Wiki < 24.2 PHP Object Injection Vulnerability

Summary
Tiki Wiki is prone to a PHP object injection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     24.2
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:       /tikiwiki
```

Solution:
Solution type: VendorFix
Update to version 24.2.

Affected Software/OS
Tiki Wiki prior to version 24.2.

Vulnerability Insight
PHP object injection in tikiimporter_blog_wordpress.php script when importing data from WordPress sites through Tiki importer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki < 24.2 PHP Object Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.127301
Version used: `2023-10-13T05:06:10Z`

References
```
cve: CVE-2023-22851
url: https://karmainsecurity.com/KIS-2023-04
```

[return to 172.20.10.3]

2.1.4 High 80/tcp

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

Summary
The Tiki Wiki CMS Groupware version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Quality of Detection (QoD): 80%

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
An EOL 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 an EOL version is present on the target host.
Details: `Tiki Wiki CMS Groupware End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.108622
Version used: `2023-09-19T05:06:03Z`

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

High (CVSS: 9.8)
NVT: Joomla! < 3.9.7 Multiple Vulnerabilities

Summary
Joomla! is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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.

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

Version used: `2023-01-31T10:08:41Z`

References

```
cve: CVE-2019-12764
cve: CVE-2019-12765
cve: CVE-2019-12766
url: https://developer.joomla.org/security-centre/785-20190603-core-acl-hardenin
↪g-of-com-joomlaupdate
url: http://www.securityfocus.com/bid/108729
url: http://www.securityfocus.com/bid/108735
url: http://www.securityfocus.com/bid/108736
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: 9.8)

NVT: Joomla! < 3.8.0 LDAP Information Disclosure Vulnerability

Summary

Joomla is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

Version used: `2023-07-14T16:09:27Z`

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
```

High (CVSS: 9.8)

NVT: Joomla < 3.9.5 Multiple Vulnerabilities

Summary

Joomla! is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

Version used: `2021-09-02T13:01:30Z`

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: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-0239
cert-bund: WID-SEC-2022-1948
cert-bund: WID-SEC-2022-1947
cert-bund: WID-SEC-2022-0732
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K21/1083
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-K19/0329
cert-bund: CB-K19/0287
dfn-cert: DFN-CERT-2023-2027
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-0481
dfn-cert: DFN-CERT-2023-0245
dfn-cert: DFN-CERT-2022-2467
dfn-cert: DFN-CERT-2021-1536
dfn-cert: DFN-CERT-2021-1503
dfn-cert: DFN-CERT-2021-0826
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-0723
```

High (CVSS: 9.8)
NVT: Joomla! Core LDAP Information Disclosure Vulnerability (Nov 2017)

Summary
Joomla is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

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 (Nov 2017)`
OID:1.3.6.1.4.1.25623.1.0.811896
Version used: `2024-02-20T05:05:48Z`

References

```
cve: CVE-2017-14596
url: https://developer.joomla.org/security-centre/714-20171101-core-ldap-informa
↪tion-disclosure.html
url: http://www.securityfocus.com/bid/100898
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
```

High (CVSS: 9.8)
NVT: Joomla < 3.8.12 Multiple Vulnerabilities

Summary
Joomla is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

Solution:
Solution type: VendorFix
Update 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
Version used: `2021-09-29T12:07:39Z`

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
```

High (CVSS: 8.8)
NVT: Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability

. . . continues on next page . . .

. . . continued from previous page . . .

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     17.2
```

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141885
Version used: `2023-07-14T16:09:27Z`

References

```
cve: CVE-2018-20719
url: https://blog.ripstech.com/2018/scan-verify-patch-security-issues-in-minutes
↪/
```

High (CVSS: 8.8)
NVT: Tiki Wiki < 24.1 Multiple Vulnerabilities

Summary
Tiki Wiki is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     24.1
Installation
path / port:       /tikiwiki
```

Solution:
Solution type: VendorFix
Update to version 24.1.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Tiki Wiki prior to version 24.1.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2023-22850: PHP object injection in /lib/sheet/grid.php
- CVE-2023-22853: PHP code injection in /lib/structures/structlib.php

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki < 24.1 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.127300
Version used: `2023-10-13T05:06:10Z`

References
```
cve: CVE-2023-22850
cve: CVE-2023-22853
url: https://karmainsecurity.com/KIS-2023-03
url: https://karmainsecurity.com/KIS-2023-02
```

High (CVSS: 8.8)
NVT: Tiki Wiki < 22 Multiple Vulnerabilities

Summary
Tiki Wiki is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.9.5
Fixed version:     22
Installation
path / port:       /tikiwiki
```

Impact
- Local (php) File Inclusion: The config file displays TikiWikis database credentials in cleartext.
- Cross-Site Request Forgery (CSRF): A successful exploit could allow the attacker to perform arbitrary actions on an affected system with the privileges of the user. These action include allowing attackers to submit their own code through an authenticated user resulting in local file Inclusion. If an authenticated user who is able to edit Tiki Wiki templates visits an malicious website, template code can be edited.
- Information Exposure: The User can authenticate against it and simply give itself admin privileges or compromise the administrator account.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Update to version 22 which disables and hides the risky preferences by default.

Affected Software/OS
Tiki Wiki through version 21.2 and probably prior.

Vulnerability Insight
The following flaws exist:
- Local (php) File Inclusion: In TikiWiki, an user can be given the permission to edit .tpl templates. This feature can be abused to escalate the users privileges by inserting the following pieceof smarty code: }include file='../db/local.php'}. The code snippet includes Tiki Wikis database configuration file and displays it in the pages source code. Any other www-data readable file like '/etc/passwd' can be included as well.
- Cross-Site Request Forgery (CSRF): Tiki Wiki allows templates to be edited without CSRF protection. This could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to follow a maliciously crafted link. (CVE-2020-29254)
- Information Exposure: An user who is able to edit template files can use smarty code to include Files like the database configuration file which allows access to TikiWikis Database.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki < 22 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.144911
Version used: `2024-06-28T05:05:33Z`

References
```
cve: CVE-2020-29254
url: https://doc.tiki.org/CVE-2020-29254
url: https://github.com/S1lkys/CVE-2020-29254
url: https://github.com/S1lkys/CVE-2020-29254/blob/main/Tiki-Wiki%2021.2%20by%20
↪Maximilian%20Barz.pdf
```

High (CVSS: 8.8)
NVT: OrangeHRM <= 4.3.1 RCE Vulnerability

Summary
OrangeHRM is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 2.4.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      4.3.2
Installation
path / port:        /orangehrm
```

Impact
Successful exploitation would allow an authenticated attacker to execute arbitrary code on the target machine.

Solution:
Solution type: VendorFix
Update to version 4.3.2 or later.

Affected Software/OS
OrangeHRM through version 4.3.1.

Vulnerability Insight
The vulnerability exists due to an input validation error within admin/listMailConfiguration (txtSendmailPath parameter).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OrangeHRM <= 4.3.1 RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113416
Version used: `2024-05-30T05:05:32Z`

References
```
cve: CVE-2019-12839
url: https://github.com/orangehrm/orangehrm/releases/tag/4.3.2
url: https://ctrsec.io/research/2019/06/12/ace-orangehrm.html
url: https://github.com/orangehrm/orangehrm/pull/528
```

High (CVSS: 8.8)
NVT: Joomla! < 3.8.13 ACL Violation Vulnerability

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.

Quality of Detection (QoD): 80%

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
Version used: `2023-07-20T05:05:17Z`

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
```

High (CVSS: 8.8)
NVT: Joomla! < 3.9.13 Multiple Vulnerabilities

Summary
Joomla! is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

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
Joomla! through version 3.9.12.

. . . continues on next page . . .

. . . continued from previous page . . .

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

Version used: `2021-09-02T13:01:30Z`

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
```

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

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

Quality of Detection (QoD): 80%

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.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.

Vulnerability Detection Method

Details: `Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100537
Version used: `2024-03-01T14:37:10Z`

References

```
cve: CVE-2010-1135
cve: CVE-2010-1134
cve: CVE-2010-1133
cve: CVE-2010-1136
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: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability

Summary

Tiki Wiki CMS Groupware is prone to a local file inclusion vulnerability.

Quality of Detection (QoD): 80%

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Insight

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

Vulnerability Detection Method

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

Details: `Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.108064

Version used: `2024-03-01T14:37:10Z`

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/
```

High (CVSS: 7.5)

NVT: HTTP Brute Force Logins With Default Credentials Reporting

Summary

It was possible to login into the remote Web Application using default credentials.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

```
It was possible to login with the following credentials (<URL>:<User>:<Password>
↪:<HTTP status code>)
http://172.20.10.3/WebGoat/attack:user:user:HTTP/1.1 200 OK
```

Impact

This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Insight

As the VT 'HTTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Reports default credentials detected by the VT 'HTTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108041).
Details: `HTTP Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103240
Version used: `2022-08-04T13:37:02Z`

References

```
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
```

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

Summary
Joomla! is prone to multiple security vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.5.15
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
Joomla! versions prior to 1.6.1.

Vulnerability Insight
The following flaws exist:
- An SQL-injection issue
- A path-disclosure vulnerability
- Multiple cross-site scripting issues
- Multiple information-disclosure vulnerabilities
- A URI-redirection vulnerability

. . . continues on next page . . .

. . . continued from previous page . . .

- A security-bypass vulnerability
- A cross-site request-forgery vulnerability
- A denial-of-service vulnerability

Vulnerability Detection Method

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

Details: `Joomla! < 1.6.1 Multiple Security Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.103114

Version used: `2022-07-22T10:11:18Z`

References

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

High (CVSS: 7.2)

NVT: Tiki Wiki < 24.2 PHP Object Injection Vulnerability

Summary

Tiki Wiki is prone to a PHP object injection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     24.2
Installation
path / port:       /tikiwiki
```

Solution:

Solution type: VendorFix

Update to version 24.2.

Affected Software/OS

Tiki Wiki prior to version 24.2.

Vulnerability Insight

PHP object injection in tikiimporter_blog_wordpress.php script when importing data from WordPress sites through Tiki importer.

Vulnerability Detection Method

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

Details: `Tiki Wiki < 24.2 PHP Object Injection Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.127301

Version used: `2023-10-13T05:06:10Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2023-22851
url: https://karmainsecurity.com/KIS-2023-04
```

[return to 172.20.10.3]

2.1.5 Medium 8080/tcp

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

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

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
The following default files were found :
http://172.20.10.3:8080/examples/servlets/index.html
http://172.20.10.3:8080/examples/jsp/snp/snoop.jsp
http://172.20.10.3:8080/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
Version used: `2023-08-01T13:29:10Z`

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following URLs requires Basic Authentication (URL:realm name):
http://172.20.10.3:8080/host-manager/html:"Tomcat Host Manager Application"
http://172.20.10.3:8080/manager/html:"Tomcat Manager Application"
http://172.20.10.3:8080/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

Version used: `2023-09-07T05:05:21Z`

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 172.20.10.3]

2.1.6 Medium 8081/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.7.2
Fixed version:     1.9.0
Installation
path / port:       /admin/../js/jquery-1.7.2.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://172.20.10.3:8081/admin/../js/jquery-1.7.2.min.js
- Referenced at:   http://172.20.10.3:8081/admin/
```

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

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
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 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
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

[return to 172.20.10.3]

2.1.7 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                       | Reason
-------------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2024-06-14T05:05:48Z`

References

```
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5
```

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

Summary

The remote SSH server is configured to allow / support weak host key algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
---------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

Solution:

Solution type: Mitigation

Disable the reported weak host key algorithm(s).

Vulnerability Detection Method

Checks the supported host key algorithms of the remote SSH server.

Currently weak host key algorithms are defined as the following:

- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)

Details: `Weak Host Key Algorithm(s) (SSH)`

OID:1.3.6.1.4.1.25623.1.0.117687

Version used: `2024-06-14T05:05:48Z`

References

```
url: https://www.rfc-editor.org/rfc/rfc8332
url: https://www.rfc-editor.org/rfc/rfc8709
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6
```

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

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.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Method

Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak encryption algorithms are defined as the following:

- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms

Details: `Weak Encryption Algorithm(s) Supported (SSH)`

OID:1.3.6.1.4.1.25623.1.0.105611

Version used: `2024-06-14T05:05:48Z`

References

```
url: https://www.rfc-editor.org/rfc/rfc8758
url: https://www.kb.cert.org/vuls/id/958563
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3
```

[return to 172.20.10.3]

2.1.8 Medium 443/tcp

Medium (CVSS: 6.8)

NVT: OrangeHRM <= 2.6.1 'uri' Parameter LFI Vulnerability

Summary

OrangeHRM is prone to a local file include (LFI) vulnerability because it fails to properly sanitize user-supplied input.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 2.4.2
Fixed version:     None
Installation
path / port:       /orangehrm
```

Impact

An attacker can exploit this vulnerability to obtain potentially sensitive information or to execute arbitrary local scripts in the context of the webserver process.

This may allow the attacker to compromise the application and the computer. Other attacks are also possible.

Solution:

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

... continues on next page ...

. . . continued from previous page . . .

Affected Software/OS
OrangeHRM version 2.6.1 is known to be vulnerable. Other versions may also be affected.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OrangeHRM <= 2.6.1 'uri' Parameter LFI Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100851
Version used: `2024-05-30T05:05:32Z`

References
```
cve: CVE-2010-4798
url: https://web.archive.org/web/20210227220254/http://www.securityfocus.com/bid
↪/43905
```

Medium (CVSS: 6.5)
NVT: Tiki Wiki < 18.10, 21.x < 21.8, 24.x < 24.3, 25.0 Multiple CSRF Vulnerabilities

Summary
Tiki Wiki is prone to multiple cross-site request forgery (CSRF) vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.9.5
Fixed version:     18.10
Installation
path / port:       /tikiwiki
```

Impact
An attacker might force an authenticated user to import arbitrary sheets or arbitrary content into Tiki Wiki by tricking a victim user into browsing to a specially crafted web page.

Solution:
Solution type: VendorFix
Update to version 18.10, 21.8, 24.3, 25.1 or later.

Affected Software/OS
Tiki Wiki prior to version 18.10, starting from 19.x and prior to 21.8, starting from 22.x and prior to 24.3 and 25.0.

Vulnerability Insight
The following vulnerabilities exist:
- CSRF in the /tiki-importer.php

. . . continues on next page . . .

. . . continued from previous page . . .

- CSRF in the /tiki-import_sheet.php

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki < 18.10, 21.x < 21.8, 24.x < 24.3, 25.0 Multiple CSRF Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.127302
Version used: `2024-01-18T05:07:09Z`

References

```
cve: CVE-2023-22852
url: https://karmainsecurity.com/KIS-2023-01
url: https://tiki.org/article499-New-Security-Updates-Released-and-Strongly-Reco
↪mmended
```

Medium (CVSS: 6.4)
NVT: Joomla! Open Redirect Vulnerability (20240202)

Summary
Joomla! is prone to an open redirect vulnerability in the installation application.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.10.15
Installation
path / port:       /joomla
```

Solution:
Solution type: VendorFix
Update to version 3.10.15, 4.4.3, 5.0.3 or later.

Affected Software/OS
Joomla! version 1.5.0 through 3.10.14, 4.0.0 through 4.4.2 and 5.0.0 through 5.0.2.

Vulnerability Insight
Inadequate parsing of URLs could result into an open redirect.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Joomla! Open Redirect Vulnerability (20240202)`
OID:1.3.6.1.4.1.25623.1.0.151798
Version used: `2024-02-23T14:36:45Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2024-21723
url: https://developer.joomla.org/security-centre/926-20240202-core-open-redirec
↪t-in-installation-application.html
cert-bund: WID-SEC-2024-0430
dfn-cert: DFN-CERT-2024-0450
```

Medium (CVSS: 6.3)
NVT: Joomla! <= 3.9.19 Multiple Vulnerabilities

Summary
Joomla! is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

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)

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Joomla! <= 3.9.19 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.113726
Version used: `2021-07-22T11:01:40Z`

References

```
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: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /mutillidae/javascript/ddsmoothmenu/jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://172.20.10.3/mutillidae/javascript/ddsmoothmenu/jquery
↪.min.js
- Referenced at:   https://172.20.10.3/mutillidae/
```

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 Insight
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 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
Version used: `2023-07-14T05:06:08Z`

References
```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.8.2
Fixed version:     1.9.0
Installation
path / port:       /owaspbricks/javascripts/jquery.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://172.20.10.3/owaspbricks/javascripts/jquery.js
- Referenced at:   https://172.20.10.3/owaspbricks/
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
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 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
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: Joomla 'Media Manager' XSS Vulnerability (20180509)

Summary
Joomla is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attackers to conduct XSS attack.

Solution:

Solution type: VendorFix

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

Affected Software/OS

Joomla 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 'Media Manager' XSS Vulnerability (20180509)`

OID:1.3.6.1.4.1.25623.1.0.813406

Version used: `2021-09-29T12:07:39Z`

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: 6.1)

NVT: Joomla 'Uri' class XSS Vulnerability

Summary

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

Quality of Detection (QoD): 80%

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

. . . continues on next page . . .

. . . continued from previous page . . .

Update to version 3.8.4 or later.

Affected Software/OS
Joomla 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
Version used: `2021-09-29T12:07:39Z`

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: 6.1)
NVT: Joomla! Core Cross-Site Scripting Vulnerability (Jul 2017)

Summary
Joomla is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

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.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

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 (Jul 2017)`
OID:1.3.6.1.4.1.25623.1.0.811257
Version used: `2024-02-19T05:05:57Z`

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: 6.1)
NVT: Joomla! Information Disclosure and Cross-Site Scripting Vulnerabilities

Summary

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

Quality of Detection (QoD): 80%

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

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.

. . . continues on next page . . .

... continued from previous page ...

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

Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2017-7983
cve: CVE-2017-7986
cve: CVE-2017-7985
url: https://developer.joomla.org/security-centre/686-20170404-core-xss-vulnerab
↪ility
url: http://www.securityfocus.com/bid/98016
url: http://www.securityfocus.com/bid/98024
url: http://www.securityfocus.com/bid/98020
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: 6.1)
NVT: Tiki Wiki < 21.2 XSS Vulnerability

Summary

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

Quality of Detection (QoD): 80%

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.

... continues on next page ...

. . . continued from previous page . . .

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
Version used: `2021-07-05T11:01:33Z`

References

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

Medium (CVSS: 6.1)
NVT: Tiki Wiki CMS Groupware < 21.0 XSS Vulnerability

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

Quality of Detection (QoD): 80%

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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

Version used: `2021-07-05T11:01:33Z`

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: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://172.20.10.3/jquery.min.js
- Referenced at:   https://172.20.10.3/
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

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 Method

. . . continues on next page . . .

. . . continued from previous page . . .

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
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary

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

Quality of Detection (QoD): 98%

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

. . . continues on next page . . .

. . . continued from previous page . . .

- Any other cipher is considered as strong

Vulnerability Detection Method

Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2024-06-14T05:05:48Z`

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-K21/0067
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
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
```

. . . continues on next page . . .

... continued from previous page ...

```
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-2023-2939
dfn-cert: DFN-CERT-2021-0775
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
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
```

... continues on next page ...

. . . continued from previous page . . .

```
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: 5.9)
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.

Quality of Detection (QoD): 98%

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 Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.8020
↪67) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

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

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

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

Vulnerability Detection Method

Check the used SSL protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: `2024-06-14T05:05:48Z`

References

```
cve: CVE-2016-0800
cve: CVE-2014-3566
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://drownattack.com/
url: https://www.imperialviolet.org/2014/10/14/poodle.html
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-0431
cert-bund: WID-SEC-2023-0427
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

Summary
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.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2023-08-01T13:29:10Z`

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
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.securityfocus.com/bid/11604
url: http://www.securityfocus.com/bid/15222
url: http://www.securityfocus.com/bid/19915
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

Medium (CVSS: 5.4)
NVT: Tiki Wiki CMS Groupware XSS Vulnerability

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

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

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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Tiki Wiki CMS Groupware XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.140797
Version used: `2023-07-20T05:05:18Z`

References

```
cve: CVE-2018-7188
url: http://openwall.com/lists/oss-security/2018/02/16/1
```

Medium (CVSS: 5.4)
NVT: Tiki Wiki CMS Groupware 18.4 XSS Vulnerability

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

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

Quality of Detection (QoD): 80%

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

Version used: `2021-08-27T13:01:16Z`

References

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

Medium (CVSS: 5.3)

NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

Summary

The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00E6870DDD72C2B9E7:CN=owaspbwa (Server certificate)
```

Impact

Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

Solution:

Solution type: Mitigation

Replace the certificate with a stronger key and reissue the certificates it signed.

Vulnerability Insight

SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

Vulnerability Detection Method

Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.

Details: `SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.150710

Version used: `2021-12-10T12:48:00Z`

References

`url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf`

Medium (CVSS: 5.3)

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.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The following files were identified:
https://172.20.10.3/cyclone/.DS_Store
https://172.20.10.3/cyclone/uploads/.DS_Store
```

Solution:

Solution type: Workaround

Block access to hidden files (starting with a dot) within your webservers configuration

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: MacOS X Finder '.DS_Store' Information Disclosure

OID:1.3.6.1.4.1.25623.1.0.10756

Version used: 2023-08-01T13:29:10Z

References

```
cve: CVE-2016-1776
cve: CVE-2018-6470
url: http://www.securityfocus.com/bid/3316
url: http://www.securityfocus.com/bid/3324
url: http://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: 5.3)

NVT: phpinfo() Output Reporting (HTTP)

Summary

Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
https://172.20.10.3/bWAPP/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/apache2 </td></tr>
  <h2>PHP Variables</h2>
https://172.20.10.3/mutillidae/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/apache2 </td></tr>
  <h2>PHP Variables</h2>
https://172.20.10.3/vicnum/test.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪p5/apache2 </td></tr>
  <h2>PHP Variables</h2>
https://172.20.10.3/vicnum/test.php?mode=phpinfo
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/apache2 </td></tr>
  <h2>PHP Variables</h2>
```

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.

Affected Software/OS

All systems exposing a file containing the output of the phpinfo() PHP function.
This VT is also reporting if an affected endpoint for the following products have been identified:
- CVE-2008-0149: TUTOS
- CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK

Vulnerability Insight

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 Method

This script reports files identified by the following separate VT: 'phpinfo() Output Detection (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.108474).
Details: `phpinfo() Output Reporting (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `2023-12-14T08:20:35Z`

References

```
cve: CVE-2008-0149
cve: CVE-2023-49282
cve: CVE-2023-49283
url: https://www.php.net/manual/en/function.phpinfo.php
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

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

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
The certificate of the remote service expired on 2022-12-31 21:12:38.
Certificate details:
fingerprint (SHA-1)             | E469E1F2987740C33AECEE7CF630CA1931BE05AE
fingerprint (SHA-256)           | B0945E8208949294EC14B1FCD2998BF148333EBB7D3413
↪5188E298B4FE2D46B2
issued by                       | CN=owaspbwa
public key algorithm            | RSA
public key size (bits)          | 1024
serial                          | 00E6870DDD72C2B9E7
signature algorithm             | sha1WithRSAEncryption
subject                         | CN=owaspbwa
subject alternative names (SAN) | None
valid from                      | 2013-01-02 21:12:38 UTC
valid until                     | 2022-12-31 21:12:38 UTC
```

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

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

Vulnerability Detection Method
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2024-06-14T05:05:48Z`

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

Summary
Tiki Wiki CMS Groupware is prone to an input sanitation weakness vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

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

Impact

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

Solution:

Solution type: VendorFix

Upgrade to version 2.2 or later.

Affected Software/OS

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

Vulnerability Insight

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

Vulnerability Detection Method

Details: `Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.800315

Version used: `2024-03-01T14:37:10Z`

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: Source Control Management (SCM) Files/Folders Accessible (HTTP)

Summary

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The following SCM files/folders were identified:
Match:      SQLite format 3
Used regex: SQLite format
URL:        https://172.20.10.3/zapwave/.svn/wc.db
Match:      0000000000000000000000000000000000000000 ef7601a2dd096f47dd1db04daf0
↪2649453a73a02 OWASP BWA <root@brokenwebapps.localdomain> 1380250028 -0400
clon
↪e: from http://git.code.sf.net/p/mutillidae/git
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
ef7601a2dd096f47dd1db04daf02649453a73a02 d4d45f1d46d0f898d927970bfc6f328cd91808b
↪d OWASP BWA <root@brokenwebapps.localdomain> 1393036379 -0500 commit: a
d4d45f1d46d0f898d927970bfc6f328cd91808bd 61753323806249c07d004b8478238043a5c7aaf
↪a OWASP BWA <root@brokenwebapps.localdomain> 1393036438 -0500 commit: a
61753323806249c07d004b8478238043a5c7aafa e62d09d3e25580bb962298eb4958bab8f081835
↪1 OWASP BWA <root@brokenwebapps.localdomain> 1393036607 -0500 commit (merge):
↪a
e62d09d3e25580bb962298eb4958bab8f0818351 779b2e292ab8bbb6023f2a4fed59cbcacb83495
↪e OWASP BWA <root@brokenwebapps.localdomain> 1394587055 -0400
pull : Merge mad
↪e by recursive.
779b2e292ab8bbb6023f2a4fed59cbcacb83495e b03f1595d1532f61a7ea5433edde87b96d038ea
↪b cwillis <chuck.willis@mandiant.com> 1430875775 -0400
commit (merge): Merge b
↪ranch 'master' of http://git.code.sf.net/p/mutillidae/git
b03f1595d1532f61a7ea5433edde87b96d038eab 2b0ee068b22cf6b6d34e25d5a8a5c2c298ad195
↪f OWASP BWA <root@brokenwebapps.localdomain> 1434677155 -0400
commit: Minor ch
↪anges for OWASPBWA VM
2b0ee068b22cf6b6d34e25d5a8a5c2c298ad195f 31eaa100cfb9f20a7590f1f7c11983284847e4d
↪7 OWASP BWA <root@brokenwebapps.localdomain> 1434677203 -0400
pull : Merge mad
↪e by recursive.
31eaa100cfb9f20a7590f1f7c11983284847e4d7 a64617c5014ae34fa28b260888c5621f2bc355b
↪e OWASP BWA <root@brokenwebapps.localdomain> 1435119130 -0400
pull : Merge mad
↪e by recursive.
a64617c5014ae34fa28b260888c5621f2bc355be f87182b59290d9accef2dfe38c2a1f4f5169708
↪b OWASP BWA <root@brokenwebapps.localdomain> 1438138113 -0400 commit (merge):
↪Merge branch 'master' of http://git.code.sf.net/p/mutillidae/git
Used regex: ^[a-f0-9]{40} [a-f0-9]{40}
URL:        https://172.20.10.3/mutillidae/.git/logs/HEAD
Match:      [core]
[remote "origin"]
[branch "master"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:        https://172.20.10.3/mutillidae/.git/config
Match:      DIRC
Used regex: ^DIRC
URL:        https://172.20.10.3/mutillidae/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
Used regex: ^Unnamed repository
URL:        https://172.20.10.3/mutillidae/.git/description
Match:      1d845f79ee4ebf9b5fbe1ee5a2aa68cc5abb6e5a branch 'master' of http://
↪git.code.sf.net/p/mutillidae/git
Used regex: ^[a-f0-9]{40}\s+(not-for-merge\s+)?branch
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
URL:        https://172.20.10.3/mutillidae/.git/FETCH_HEAD
Match:      f87182b59290d9accef2dfe38c2a1f4f5169708b
Used regex: ^[a-f0-9]{40}$
URL:        https://172.20.10.3/mutillidae/.git/ORIG_HEAD
Match:      ref: refs/heads/master
Used regex: ^ref: refs/
URL:        https://172.20.10.3/mutillidae/.git/HEAD
Match:      0000000000000000000000000000000000000000 f65b94248fb6db12561653121ab
↪5c80acad07de0 OWASP BWA <root@brokenwebapps.localdomain> 1434679952 -0400
clon
↪e: from https://github.com/SpiderLabs/MCIR.git
f65b94248fb6db12561653121ab5c80acad07de0 997b6f1fca1a40f264f742ef3d5faee2a74fb68
↪e OWASP BWA <root@brokenwebapps.localdomain> 1434682047 -0400 commit: Changed
↪database connection info for OWASPBWA VM
Used regex: ^[a-f0-9]{40} [a-f0-9]{40}
URL:        https://172.20.10.3/MCIR/.git/logs/HEAD
Match:      [core]
[remote "origin"]
[branch "master"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:        https://172.20.10.3/MCIR/.git/config
Match:      DIRC
Used regex: ^DIRC
URL:        https://172.20.10.3/MCIR/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
Used regex: ^Unnamed repository
URL:        https://172.20.10.3/MCIR/.git/description
Match:      f65b94248fb6db12561653121ab5c80acad07de0 branch 'master' of https:/
↪/github.com/SpiderLabs/MCIR
Used regex: ^[a-f0-9]{40}\s+(not-for-merge\s+)?branch
URL:        https://172.20.10.3/MCIR/.git/FETCH_HEAD
Match:      997b6f1fca1a40f264f742ef3d5faee2a74fb68e
Used regex: ^[a-f0-9]{40}$
URL:        https://172.20.10.3/MCIR/.git/ORIG_HEAD
Match:      ref: refs/heads/master
Used regex: ^ref: refs/
URL:        https://172.20.10.3/MCIR/.git/HEAD
Match:      0000000000000000000000000000000000000000 b9f730196f5743225c70dd3ee33
↪7fe6b325e32ce OWASP BWA <root@brokenwebapps.localdomain> 1373503332 -0400
clon
↪e: from https://github.com/RandomStorm/DVWA.git
b9f730196f5743225c70dd3ee337fe6b325e32ce 6040830f6eaec1c67dc7bdd98b2da13c51c41c8
↪3 OWASP BWA <root@brokenwebapps.localdomain> 1431657172 -0400
pull : Fast-forw
↪ard
Used regex: ^[a-f0-9]{40} [a-f0-9]{40}
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
URL:        https://172.20.10.3/dvwa/.git/logs/HEAD
Match:      [core]
[remote "origin"]
[branch "master"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:        https://172.20.10.3/dvwa/.git/config
Match:      DIRC
Used regex: ^DIRC
URL:        https://172.20.10.3/dvwa/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
Used regex: ^Unnamed repository
URL:        https://172.20.10.3/dvwa/.git/description
Match:      6040830f6eaec1c67dc7bdd98b2da13c51c41c83 branch 'master' of https:/
↪/github.com/RandomStorm/DVWA
Used regex: ^[a-f0-9]{40}\s+(not-for-merge\s+)?branch
URL:        https://172.20.10.3/dvwa/.git/FETCH_HEAD
Match:      6040830f6eaec1c67dc7bdd98b2da13c51c41c83
Used regex: ^[a-f0-9]{40}$
URL:        https://172.20.10.3/dvwa/.git/ORIG_HEAD
Match:      ref: refs/heads/master
Used regex: ^ref: refs/
URL:        https://172.20.10.3/dvwa/.git/HEAD
```

Impact

Based on the information provided in these files/folders 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 SCM files/folders for authorized systems only.

Vulnerability Insight

Currently the script is checking for files/folders of the following SCM software:

- Git (.git)
- Mercurial (.hg)
- Bazaar (.bzr)
- CVS (CVS/Root, CVS/Entries)
- Subversion (.svn)

Vulnerability Detection Method

Check the response if SCM files/folders are accessible.

Details: `Source Control Management (SCM) Files/Folders Accessible (HTTP)`

OID:1.3.6.1.4.1.25623.1.0.111084

Version used: `2023-08-01T13:29:10Z`

. . . continues on next page . . .

. . . continued from previous page . . .

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: WordPress < 6.5 Private Information Exposure Vulnerability

Summary

WordPress is prone to a private information exposure via 'redirect_guess_404_permalink()'.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 2.0
Fixed version:     6.5
Installation
path / port:       /wordpress
```

Impact

This can allow unauthenticated attackers to expose the slug of a custom post whose 'publicly_queryable' post status has been set to 'false'.

Solution:

Solution type: VendorFix

Update to version 6.5 or later.

Note: As of 04/2024 the security fix is only available in version 6.5 and haven't been 'backported' to older versions yet.

Affected Software/OS

WordPress versions prior to 6.5.

Vulnerability Insight

When guessing the proper URL to redirect a 404, WordPress only considers the post statuses and not the proper post type privacy settings, leading to potential information disclosure.

Vulnerability Detection Method

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

Details: `WordPress < 6.5 Private Information Exposure Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.114477

Version used: `2024-04-10T05:05:22Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2023-5692
url: https://core.trac.wordpress.org/ticket/59795
url: https://core.trac.wordpress.org/changeset/57645
url: https://bugzilla.redhat.com/show_bug.cgi?id=2273662
url: https://www.wordfence.com/threat-intel/vulnerabilities/id/6e6f993b-ce09-405
↪0-84a1-cbe9953f36b1
url: https://patchstack.com/database/vulnerability/wordpress/wordpress-wordpress
↪-core-plugin-6-4-3-sensitive-information-exposure-via-redirect-guess-404-perma
↪link-vulnerability
cert-bund: WID-SEC-2024-0808
```

Medium (CVSS: 4.3)
NVT: OrangeHRM <= 2.6.2 'jobVacancy.php' XSS Vulnerability - Active Check

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
Vulnerable URL: https://172.20.10.3/orangehrm/templates/recruitment/jobVacancy.p
↪hp?recruitcode=</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
OrangeHRM version 2.6.2 is known to be vulnerable. Other versions may also be affected.

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `OrangeHRM <= 2.6.2 'jobVacancy.php' XSS Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.103132
Version used: `2024-05-30T05:05:32Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
url: https://web.archive.org/web/20210127124242/http://www.securityfocus.com/bid
↪/47046
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The service is only providing the deprecated TLSv1.0 protocol and supports one o
↪r more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report S
↪upported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-06-14T05:05:48Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

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

Summary
Tiki Wiki CMS Groupware is prone to Multiple Cross Site Scripting vulnerabilities.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
Vulnerable URL: https://172.20.10.3/tikiwiki/tiki-listpages.php/<script>alert("X
↪SS_Check");</script>
```

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

Solution:
Solution type: VendorFix
Upgrade to Tiki Wiki CMS Groupware version 2.4 or later.

Affected Software/OS
Tiki Wiki CMS Groupware version 2.2, 2.3 and prior.

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

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `Tiki Wiki CMS Groupware Multiple Cross Site Scripting Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800266
Version used: `2023-10-27T05:05:28Z`

References

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

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

Summary

A weakness has been discovered in the Apache HTTP Server if configured to use the FileETag directive.

Quality of Detection (QoD): 80%

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 HTTP Server 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 HTTP Server ETag Header Information Disclosure Weakness`
OID:1.3.6.1.4.1.25623.1.0.103122

. . . continues on next page . . .

... continued from previous page ...

Version used: 2022-12-05T10:11:03Z

References

```
cve: CVE-2003-1418
url: http://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: jQuery < 1.6.3 XSS Vulnerability

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
path / port:       /jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://172.20.10.3/jquery.min.js
- Referenced at:   https://172.20.10.3/
```

Solution:

Solution type: VendorFix

Update to version 1.6.3 or later.

Affected Software/OS

jQuery prior to version 1.6.3.

Vulnerability Insight

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 Method

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

... continues on next page ...

. . . continued from previous page . . .

Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

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: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary
Apache HTTP Server is prone to a cookie information disclosure vulnerability.

Quality of Detection (QoD): 99%

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

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

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

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21.

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

Vulnerability Detection Method
Details: `Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: `2022-04-27T12:01:52Z`

References

```
cve: CVE-2012-0053
url: http://secunia.com/advisories/47779
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/51706
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
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188
```

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

Summary
Joomla is prone to multiple Cross-site scripting vulnerabilities.

Quality of Detection (QoD): 80%

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
Version used: `2024-03-04T14:37:58Z`

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: jQuery < 1.6.3 XSS Vulnerability

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
path / port:       /mutillidae/javascript/ddsmoothmenu/jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: https://172.20.10.3/mutillidae/javascript/ddsmoothmenu/jquery
↪.min.js
- Referenced at:   https://172.20.10.3/mutillidae/
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

jQuery prior to version 1.6.3.

Vulnerability Insight

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 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
Version used: `2023-07-14T05:06:08Z`

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: 4.0)
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.

Quality of Detection (QoD): 80%

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)

. . . continues on next page . . .

. . . continued from previous page . . .

- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

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

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

Fingerprint1

or

fingerprint1, Fingerprint2

Vulnerability Detection Method

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`

OID:1.3.6.1.4.1.25623.1.0.105880

Version used: `2021-10-15T11:13:32Z`

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).

Quality of Detection (QoD): 80%

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Method

Checks the DHE temporary public key size.

Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.106223

Version used: `2023-07-21T05:05:22Z`

References

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

[return to 172.20.10.3]

2.1.9 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: OrangeHRM <= 2.6.1 'uri' Parameter LFI Vulnerability

Summary

OrangeHRM is prone to a local file include (LFI) vulnerability because it fails to properly sanitize user-supplied input.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 2.4.2
Fixed version:     None
Installation
path / port:       /orangehrm
```

Impact

An attacker can exploit this vulnerability to obtain potentially sensitive information or to execute arbitrary local scripts in the context of the webserver process.

This may allow the attacker to compromise the application and the computer. Other attacks are also possible.

Solution:

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
OrangeHRM version 2.6.1 is known to be vulnerable. Other versions may also be affected.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OrangeHRM <= 2.6.1 'uri' Parameter LFI Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100851
Version used: `2024-05-30T05:05:32Z`

References

```
cve: CVE-2010-4798
url: https://web.archive.org/web/20210227220254/http://www.securityfocus.com/bid
↪/43905
```

Medium (CVSS: 6.8)
NVT: WebCalendar < 1.2.1 Multiple CSS and CSRF Vulnerabilities

Summary
WebCalendar is prone to multiple CSS and CSRF Vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.0.3
Fixed version:     1.2.1
Installation
path / port:       /webcal
```

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

Solution:
Solution type: VendorFix
Update version 1.2.1 or later.

Affected Software/OS
WebCalendar version 1.2.0 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- Input passed to the 'tab' parameter in 'users.php' is not properly sanitised before being returned to the user.

. . . continues on next page . . .

. . . continued from previous page . . .

- 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

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

Details: `WebCalendar < 1.2.1 Multiple CSS and CSRF Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.800472

Version used: `2023-12-20T05:05:58Z`

References

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

Medium (CVSS: 6.5)

NVT: Tiki Wiki < 18.10, 21.x < 21.8, 24.x < 24.3, 25.0 Multiple CSRF Vulnerabilities

Summary

Tiki Wiki is prone to multiple cross-site request forgery (CSRF) vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.9.5
Fixed version:     18.10
Installation
path / port:       /tikiwiki
```

Impact

An attacker might force an authenticated user to import arbitrary sheets or arbitrary content into Tiki Wiki by tricking a victim user into browsing to a specially crafted web page.

Solution:

Solution type: VendorFix

Update to version 18.10, 21.8, 24.3, 25.1 or later.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Tiki Wiki prior to version 18.10, starting from 19.x and prior to 21.8, starting from 22.x and prior to 24.3 and 25.0.

Vulnerability Insight

The following vulnerabilities exist:

- CSRF in the /tiki-importer.php
- CSRF in the /tiki-import_sheet.php

Vulnerability Detection Method

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

Details: `Tiki Wiki < 18.10, 21.x < 21.8, 24.x < 24.3, 25.0 Multiple CSRF Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.127302

Version used: `2024-01-18T05:07:09Z`

References

```
cve: CVE-2023-22852
url: https://karmainsecurity.com/KIS-2023-01
url: https://tiki.org/article499-New-Security-Updates-Released-and-Strongly-Reco
↪mmended
```

Medium (CVSS: 6.4)

NVT: Joomla! Open Redirect Vulnerability (20240202)

Summary

Joomla! is prone to an open redirect vulnerability in the installation application.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.5.15
Fixed version:     3.10.15
Installation
path / port:       /joomla
```

Solution:

Solution type: VendorFix

Update to version 3.10.15, 4.4.3, 5.0.3 or later.

Affected Software/OS

Joomla! version 1.5.0 through 3.10.14, 4.0.0 through 4.4.2 and 5.0.0 through 5.0.2.

Vulnerability Insight

Inadequate parsing of URLs could result into an open redirect.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Joomla! Open Redirect Vulnerability (20240202)`
OID:1.3.6.1.4.1.25623.1.0.151798
Version used: `2024-02-23T14:36:45Z`

References

```
cve: CVE-2024-21723
url: https://developer.joomla.org/security-centre/926-20240202-core-open-redirec
↪t-in-installation-application.html
cert-bund: WID-SEC-2024-0430
dfn-cert: DFN-CERT-2024-0450
```

Medium (CVSS: 6.3)
NVT: Joomla! <= 3.9.19 Multiple Vulnerabilities

Summary
Joomla! is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

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)

. . . continues on next page . . .

. . . continued from previous page . . .

- 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
Version used: `2021-07-22T11:01:40Z`

References

```
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: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
- Identified file: http://172.20.10.3/jquery.min.js
- Referenced at:   http://172.20.10.3/
```

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

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
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 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
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.8.0
Fixed version:     1.9.0
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:       /cyclone/assets/jquery.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://172.20.10.3/cyclone/assets/jquery.js
- Referenced at:   http://172.20.10.3/cyclone/
```

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

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
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 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
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.3.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     1.9.0
Installation
path / port:       /mutillidae/javascript/ddsmoothmenu/jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://172.20.10.3/mutillidae/javascript/ddsmoothmenu/jquery.
↪min.js
- Referenced at:   http://172.20.10.3/mutillidae/
```

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

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
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 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
Version used: `2023-07-14T05:06:08Z`

References
```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.8.2
Fixed version:     1.9.0
Installation
path / port:       /owaspbricks/config/../javascripts/jquery.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://172.20.10.3/owaspbricks/config/../javascripts/jquery.j
↪s
- Referenced at:   http://172.20.10.3/owaspbricks/config/
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

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 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

Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.8.2
Fixed version:     1.9.0
Installation
path / port:       /owaspbricks/javascripts/jquery.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://172.20.10.3/owaspbricks/javascripts/jquery.js
- Referenced at:   http://172.20.10.3/owaspbricks/
```

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

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
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 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
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: Joomla 'Media Manager' XSS Vulnerability (20180509)

Summary
Joomla is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

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

Affected Software/OS
Joomla 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 'Media Manager' XSS Vulnerability (20180509)`
OID:1.3.6.1.4.1.25623.1.0.813406
Version used: `2021-09-29T12:07:39Z`

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: 6.1)
NVT: Joomla 'Uri' class XSS Vulnerability

Summary
Joomla is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

. . . continues on next page . . .

. . . continued from previous page . . .

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

Update to version 3.8.4 or later.

Affected Software/OS

Joomla 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

Version used: `2021-09-29T12:07:39Z`

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: 6.1)

NVT: Joomla! Core Cross-Site Scripting Vulnerability (Jul 2017)

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

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.

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 (Jul 2017)`
OID:1.3.6.1.4.1.25623.1.0.811257
Version used: `2024-02-19T05:05:57Z`

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: 6.1)
NVT: Joomla! Information Disclosure and Cross-Site Scripting Vulnerabilities

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

Quality of Detection (QoD): 80%

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:

. . . continues on next page . . .

. . . continued from previous page . . .

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
Version used: `2023-11-03T05:05:46Z`

References

```
cve: CVE-2017-7983
cve: CVE-2017-7986
cve: CVE-2017-7985
url: https://developer.joomla.org/security-centre/686-20170404-core-xss-vulnerab
↪ility
url: http://www.securityfocus.com/bid/98016
url: http://www.securityfocus.com/bid/98024
url: http://www.securityfocus.com/bid/98020
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: 6.1)
NVT: Tiki Wiki < 21.2 XSS Vulnerability

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.9.5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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

Version used: `2021-07-05T11:01:33Z`

References

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

Medium (CVSS: 6.1)

NVT: Tiki Wiki CMS Groupware < 21.0 XSS Vulnerability

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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
Version used: `2021-07-05T11:01:33Z`

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

Summary
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.

Quality of Detection (QoD): 99%

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2023-08-01T13:29:10Z`

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
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.securityfocus.com/bid/11604
url: http://www.securityfocus.com/bid/15222
url: http://www.securityfocus.com/bid/19915
url: http://www.securityfocus.com/bid/24456
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

Medium (CVSS: 5.4)
NVT: Tiki Wiki CMS Groupware 18.4 XSS Vulnerability

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

Quality of Detection (QoD): 80%

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
Version used: `2021-08-27T13:01:16Z`

References

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

Medium (CVSS: 5.4)
NVT: Tiki Wiki CMS Groupware XSS Vulnerability

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.

Quality of Detection (QoD): 80%

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

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

Solution:

Solution type: VendorFix

Upgrade to version 18.0 or later.

Affected Software/OS

Tiki Wiki CMS Groupware prior to version 18.0.

Vulnerability Detection Method

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

Details: `Tiki Wiki CMS Groupware XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.140797

Version used: `2023-07-20T05:05:18Z`

References

```
cve: CVE-2018-7188
url: http://openwall.com/lists/oss-security/2018/02/16/1
```

Medium (CVSS: 5.3)

NVT: phpinfo() Output Reporting (HTTP)

Summary

Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://172.20.10.3/bWAPP/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/apache2 </td></tr>
  <h2>PHP Variables</h2>
http://172.20.10.3/mutillidae/phpinfo.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪p5/apache2 </td></tr>
  <h2>PHP Variables</h2>
http://172.20.10.3/vicnum/test.php
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/apache2 </td></tr>
  <h2>PHP Variables</h2>
http://172.20.10.3/vicnum/test.php?mode=phpinfo
Concluded from:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/apache2 </td></tr>
  <h2>PHP Variables</h2>
```

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.

Affected Software/OS

All systems exposing a file containing the output of the phpinfo() PHP function.
This VT is also reporting if an affected endpoint for the following products have been identified:
- CVE-2008-0149: TUTOS
- CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK

Vulnerability Insight

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 Method

This script reports files identified by the following separate VT: 'phpinfo() Output Detection (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.108474).
Details: `phpinfo() Output Reporting (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `2023-12-14T08:20:35Z`

References

`cve: CVE-2008-0149`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2023-49282
cve: CVE-2023-49283
url: https://www.php.net/manual/en/function.phpinfo.php
```

Medium (CVSS: 5.3)
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.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The following files were identified:
http://172.20.10.3/cyclone/.DS_Store
http://172.20.10.3/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
Version used: `2023-08-01T13:29:10Z`

References

```
cve: CVE-2016-1776
cve: CVE-2018-6470
url: http://www.securityfocus.com/bid/3316
url: http://www.securityfocus.com/bid/3324
url: http://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: WordPress < 6.5 Private Information Exposure Vulnerability

Summary
WordPress is prone to a private information exposure via 'redirect_guess_404_permalink()'.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 2.0
Fixed version:     6.5
Installation
path / port:       /wordpress
```

Impact

This can allow unauthenticated attackers to expose the slug of a custom post whose 'publicly_queryable' post status has been set to 'false'.

Solution:

Solution type: VendorFix

Update to version 6.5 or later.

Note: As of 04/2024 the security fix is only available in version 6.5 and haven't been 'backported' to older versions yet.

Affected Software/OS

WordPress versions prior to 6.5.

Vulnerability Insight

When guessing the proper URL to redirect a 404, WordPress only considers the post statuses and not the proper post type privacy settings, leading to potential information disclosure.

Vulnerability Detection Method

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

Details: `WordPress < 6.5 Private Information Exposure Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.114477

Version used: `2024-04-10T05:05:22Z`

References

```
cve: CVE-2023-5692
url: https://core.trac.wordpress.org/ticket/59795
url: https://core.trac.wordpress.org/changeset/57645
url: https://bugzilla.redhat.com/show_bug.cgi?id=2273662
url: https://www.wordfence.com/threat-intel/vulnerabilities/id/6e6f993b-ce09-405
↪0-84a1-cbe9953f36b1
url: https://patchstack.com/database/vulnerability/wordpress/wordpress-wordpress
↪-core-plugin-6-4-3-sensitive-information-exposure-via-redirect-guess-404-perma
↪link-vulnerability
cert-bund: WID-SEC-2024-0808
```

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

Summary
Tiki Wiki CMS Groupware is prone to an input sanitation weakness vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

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

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

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

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

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

Vulnerability Detection Method
Details: `Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800315
Version used: `2024-03-01T14:37:10Z`

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: Source Control Management (SCM) Files/Folders Accessible (HTTP)

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
The following SCM files/folders were identified:
Match:      SQLite format 3
Used regex: SQLite format
URL:        http://172.20.10.3/zapwave/.svn/wc.db
Match:      0000000000000000000000000000000000000000 ef7601a2dd096f47dd1db04daf0
↪2649453a73a02 OWASP BWA <root@brokenwebapps.localdomain> 1380250028 -0400
clon
↪e: from http://git.code.sf.net/p/mutillidae/git
ef7601a2dd096f47dd1db04daf02649453a73a02 d4d45f1d46d0f898d927970bfc6f328cd91808b
↪d OWASP BWA <root@brokenwebapps.localdomain> 1393036379 -0500 commit: a
d4d45f1d46d0f898d927970bfc6f328cd91808bd 61753323806249c07d004b8478238043a5c7aaf
↪a OWASP BWA <root@brokenwebapps.localdomain> 1393036438 -0500 commit: a
61753323806249c07d004b8478238043a5c7aafa e62d09d3e25580bb962298eb4958bab8f081835
↪1 OWASP BWA <root@brokenwebapps.localdomain> 1393036607 -0500 commit (merge):
↪a
e62d09d3e25580bb962298eb4958bab8f0818351 779b2e292ab8bbb6023f2a4fed59cbcacb83495
↪e OWASP BWA <root@brokenwebapps.localdomain> 1394587055 -0400
pull : Merge mad
↪e by recursive.
779b2e292ab8bbb6023f2a4fed59cbcacb83495e b03f1595d1532f61a7ea5433edde87b96d038ea
↪b cwillis <chuck.willis@mandiant.com> 1430875775 -0400
commit (merge): Merge b
↪ranch 'master' of http://git.code.sf.net/p/mutillidae/git
b03f1595d1532f61a7ea5433edde87b96d038eab 2b0ee068b22cf6b6d34e25d5a8a5c2c298ad195
↪f OWASP BWA <root@brokenwebapps.localdomain> 1434677155 -0400
commit: Minor ch
↪anges for OWASPBWA VM
2b0ee068b22cf6b6d34e25d5a8a5c2c298ad195f 31eaa100cfb9f20a7590f1f7c11983284847e4d
↪7 OWASP BWA <root@brokenwebapps.localdomain> 1434677203 -0400
pull : Merge mad
↪e by recursive.
31eaa100cfb9f20a7590f1f7c11983284847e4d7 a64617c5014ae34fa28b260888c5621f2bc355b
↪e OWASP BWA <root@brokenwebapps.localdomain> 1435119130 -0400
pull : Merge mad
↪e by recursive.
a64617c5014ae34fa28b260888c5621f2bc355be f87182b59290d9accef2dfe38c2a1f4f5169708
↪b OWASP BWA <root@brokenwebapps.localdomain> 1438138113 -0400 commit (merge):
↪Merge branch 'master' of http://git.code.sf.net/p/mutillidae/git
Used regex: ^[a-f0-9]{40} [a-f0-9]{40}
URL:        http://172.20.10.3/mutillidae/.git/logs/HEAD
Match:      [core]
[remote "origin"]
[branch "master"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:        http://172.20.10.3/mutillidae/.git/config
Match:      DIRC
Used regex: ^DIRC
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
URL:        http://172.20.10.3/mutillidae/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
Used regex: ^Unnamed repository
URL:        http://172.20.10.3/mutillidae/.git/description
Match:      1d845f79ee4ebf9b5fbe1ee5a2aa68cc5abb6e5a branch 'master' of http://
↪git.code.sf.net/p/mutillidae/git
Used regex: ^[a-f0-9]{40}\s+(not-for-merge\s+)?branch
URL:        http://172.20.10.3/mutillidae/.git/FETCH_HEAD
Match:      f87182b59290d9accef2dfe38c2a1f4f5169708b
Used regex: ^[a-f0-9]{40}$
URL:        http://172.20.10.3/mutillidae/.git/ORIG_HEAD
Match:      ref: refs/heads/master
Used regex: ^ref: refs/
URL:        http://172.20.10.3/mutillidae/.git/HEAD
Match:      0000000000000000000000000000000000000000 f65b94248fb6db12561653121ab
↪5c80acad07de0 OWASP BWA <root@brokenwebapps.localdomain> 1434679952 -0400
clon
↪e: from https://github.com/SpiderLabs/MCIR.git
f65b94248fb6db12561653121ab5c80acad07de0 997b6f1fca1a40f264f742ef3d5faee2a74fb68
↪e OWASP BWA <root@brokenwebapps.localdomain> 1434682047 -0400 commit: Changed
↪database connection info for OWASPBWA VM
Used regex: ^[a-f0-9]{40} [a-f0-9]{40}
URL:        http://172.20.10.3/MCIR/.git/logs/HEAD
Match:      [core]
[remote "origin"]
[branch "master"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:        http://172.20.10.3/MCIR/.git/config
Match:      DIRC
Used regex: ^DIRC
URL:        http://172.20.10.3/MCIR/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
Used regex: ^Unnamed repository
URL:        http://172.20.10.3/MCIR/.git/description
Match:      f65b94248fb6db12561653121ab5c80acad07de0 branch 'master' of https:/
↪/github.com/SpiderLabs/MCIR
Used regex: ^[a-f0-9]{40}\s+(not-for-merge\s+)?branch
URL:        http://172.20.10.3/MCIR/.git/FETCH_HEAD
Match:      997b6f1fca1a40f264f742ef3d5faee2a74fb68e
Used regex: ^[a-f0-9]{40}$
URL:        http://172.20.10.3/MCIR/.git/ORIG_HEAD
Match:      ref: refs/heads/master
Used regex: ^ref: refs/
URL:        http://172.20.10.3/MCIR/.git/HEAD
Match:      0000000000000000000000000000000000000000 b9f730196f5743225c70dd3ee33
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪7fe6b325e32ce OWASP BWA <root@brokenwebapps.localdomain> 1373503332 -0400
clon
↪e: from https://github.com/RandomStorm/DVWA.git
b9f730196f5743225c70dd3ee337fe6b325e32ce 6040830f6eaec1c67dc7bdd98b2da13c51c41c8
↪3 OWASP BWA <root@brokenwebapps.localdomain> 1431657172 -0400
pull : Fast-forw
↪ard
Used regex: ^[a-f0-9]{40} [a-f0-9]{40}
URL:        http://172.20.10.3/dvwa/.git/logs/HEAD
Match:      [core]
[remote "origin"]
[branch "master"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:        http://172.20.10.3/dvwa/.git/config
Match:      DIRC
Used regex: ^DIRC
URL:        http://172.20.10.3/dvwa/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
Used regex: ^Unnamed repository
URL:        http://172.20.10.3/dvwa/.git/description
Match:      6040830f6eaec1c67dc7bdd98b2da13c51c41c83 branch 'master' of https:/
↪/github.com/RandomStorm/DVWA
Used regex: ^[a-f0-9]{40}\s+(not-for-merge\s+)?branch
URL:        http://172.20.10.3/dvwa/.git/FETCH_HEAD
Match:      6040830f6eaec1c67dc7bdd98b2da13c51c41c83
Used regex: ^[a-f0-9]{40}$
URL:        http://172.20.10.3/dvwa/.git/ORIG_HEAD
Match:      ref: refs/heads/master
Used regex: ^ref: refs/
URL:        http://172.20.10.3/dvwa/.git/HEAD
```

Impact

Based on the information provided in these files/folders 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 SCM files/folders for authorized systems only.

Vulnerability Insight

Currently the script is checking for files/folders of the following SCM software:

- Git (.git)
- Mercurial (.hg)
- Bazaar (.bzr)
- CVS (CVS/Root, CVS/Entries)

. . . continues on next page . . .

. . . continued from previous page . . .

- Subversion (.svn)

Vulnerability Detection Method

Check the response if SCM files/folders are accessible.
Details: `Source Control Management (SCM) Files/Folders Accessible (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.111084
Version used: `2023-08-01T13:29:10Z`

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: WebCalendar < 1.0.4 User Account Enumeration Disclosure Vulnerability - Active Check

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.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
Vulnerable URL: http://172.20.10.3/webcal/login.php
```

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

Vulnerability Detection Method

Details: `WebCalendar < 1.0.4 User Account Enumeration Disclosure Vulnerability - Active .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.80021
Version used: `2023-08-01T13:29:10Z`

References

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪0
osvdb: 25280
```

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following URLs requires Basic Authentication (URL:realm name):
http://172.20.10.3/WebGoat/attack:"WebGoat 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
Version used: `2023-09-07T05:05:21Z`

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: OrangeHRM <= 2.6.2 'jobVacancy.php' XSS Vulnerability - Active Check

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
Vulnerable URL: http://172.20.10.3/orangehrm/templates/recruitment/jobVacancy.ph
↪p?recruitcode=</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
OrangeHRM version 2.6.2 is known to be vulnerable. Other versions may also be affected.

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `OrangeHRM <= 2.6.2 'jobVacancy.php' XSS Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.103132
Version used: `2024-05-30T05:05:32Z`

References

```
url: https://web.archive.org/web/20210127124242/http://www.securityfocus.com/bid
↪/47046
```

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

Summary
Tiki Wiki CMS Groupware is prone to Multiple Cross Site Scripting vulnerabilities.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

... continues on next page ...

. . . continued from previous page . . .

```
Vulnerable URL: http://172.20.10.3/tikiwiki/tiki-listpages.php/<script>alert("XS
↪S_Check");</script>
```

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

Solution:
Solution type: VendorFix
Upgrade to Tiki Wiki CMS Groupware version 2.4 or later.

Affected Software/OS
Tiki Wiki CMS Groupware version 2.2, 2.3 and prior.

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

Vulnerability Detection Method
Details: `Tiki Wiki CMS Groupware Multiple Cross Site Scripting Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800266
Version used: `2023-10-27T05:05:28Z`

References

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

Medium (CVSS: 4.3)
NVT: WebCalendar < 1.2.4 Multiple XSS Vulnerabilities

Summary
WebCalendar is prone to multiple cross-site scripting (XSS) vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.0.3
Fixed version:     1.2.4
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

`path / port:        /webcal`

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

Update to version 1.2.4 or later.

Affected Software/OS

WebCalendar version 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

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

Details: `WebCalendar < 1.2.4 Multiple XSS Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.802305

Version used: `2023-12-20T05:05:58Z`

References

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

Medium (CVSS: 4.3)

NVT: Apache HTTP Server ETag Header Information Disclosure Weakness

Summary

A weakness has been discovered in the Apache HTTP Server if configured to use the FileETag directive.

Quality of Detection (QoD): 80%

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:

. . . continues on next page . . .

. . . continued from previous page . . .

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 HTTP Server 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 HTTP Server ETag Header Information Disclosure Weakness`
OID:1.3.6.1.4.1.25623.1.0.103122
Version used: `2022-12-05T10:11:03Z`

References

```
cve: CVE-2003-1418
url: http://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: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary
Apache HTTP Server is prone to a cookie information disclosure vulnerability.

Quality of Detection (QoD): 99%

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

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

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21.

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

Vulnerability Detection Method
Details: `Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: `2022-04-27T12:01:52Z`

References

```
cve: CVE-2012-0053
url: http://secunia.com/advisories/47779
url: http://www.securityfocus.com/bid/51706
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
dfn-cert: DFN-CERT-2012-0203
dfn-cert: DFN-CERT-2012-0188
```

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

Summary
Joomla is prone to multiple Cross-site scripting vulnerabilities.

Quality of Detection (QoD): 80%

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
Version used: `2024-03-04T14:37:58Z`

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: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
path / port:       /mutillidae/javascript/ddsmoothmenu/jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://172.20.10.3/mutillidae/javascript/ddsmoothmenu/jquery.
↪min.js
- Referenced at:   http://172.20.10.3/mutillidae/
```

Solution:

Solution type: VendorFix

Update to version 1.6.3 or later.

Affected Software/OS

jQuery prior to version 1.6.3.

Vulnerability Insight

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 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

Version used: `2023-07-14T05:06:08Z`

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 < 1.6.3 XSS Vulnerability

Summary

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 1.3.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     1.6.3
Installation
path / port:       /jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://172.20.10.3/jquery.min.js
- Referenced at:   http://172.20.10.3/
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
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 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
Version used: `2023-07-14T05:06:08Z`

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
```

[return to 172.20.10.3]

2.1.10 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 2373202
Packet 2: 2373474
```

Impact

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

Solution:

Solution type: Mitigation

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

Affected Software/OS

TCP 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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 172.20.10.3]

2.1.11 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-sha1-96
umac-64@openssh.com
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

References
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[return to 172.20.10.3]

2.1.12 Low 443/tcp

Low (CVSS: 3.4)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

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

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

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

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

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details: `SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: `2024-06-14T05:05:48Z`

References

```
cve: CVE-2014-3566
url: https://www.openssl.org/~bodo/ssl-poodle.pdf
url: http://www.securityfocus.com/bid/70574
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: WID-SEC-2023-0431
cert-bund: CB-K17/1198
cert-bund: CB-K17/1196
cert-bund: CB-K16/1828
cert-bund: CB-K16/1438
```

. . . continues on next page . . .

... continued from previous page ...

```
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
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
```

... continues on next page ...

. . . continued from previous page . . .

```
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
```

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.

Quality of Detection (QoD): 98%

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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
Version used: 2023-07-14T16:09:27Z

References

```
cve: CVE-2012-4929
cve: CVE-2012-4930
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
```

[return to 172.20.10.3]

2.1.13 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 172.20.10.3]

This file was automatically generated.