Scan Report

March 7, 2023

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 “Scan Webserver”. The scan started at Tue Mar 7 00:53:38 2023 UTC and ended at Tue Mar 7 01:04:29 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.200.0.12 www.seclab.net	5	12	1	0	0
Total: 1	5	12	1	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 18 results selected by the filtering described above. Before filtering there were 247 results.

2 Results per Host

2.1 10.200.0.12

Host scan start	Tue Mar 7 00:54:16 2023 UTC
Host scan end	Tue Mar 7 01:04:25 2023 UTC

Service (Port)	Threat Level
80/tcp	High
general/tcp	High
80/tcp	Medium
general/tcp	Low

2.1.1 High 80/tcp

High (CVSS: 10.0)
NVT: TWiki XSS and Command Execution Vulnerabilities

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

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
Installed version: 01.Feb.2003
Fixed version:     4.2.4
```

Impact

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

Solution:

Solution type: VendorFix

Upgrade to version 4.2.4 or later.

Affected Software/OS

TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight

The flaws are due to:

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

Vulnerability Detection Method

Details: `TWiki XSS and Command Execution Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.800320

Version used: `2022-05-11T11:17:52Z`

References

```
cve: CVE-2008-5304
cve: CVE-2008-5305
url: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304
url: http://www.securityfocus.com/bid/32668
url: http://www.securityfocus.com/bid/32669
url: http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305
```

High (CVSS: 7.5)

NVT: Test HTTP dangerous methods

Summary

Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.

Vulnerability Detection Result

```
We could upload the following files via the PUT method at this web server:
http://www.seclab.net/dav/puttest647009096.html
We could delete the following files via the DELETE method at this web server:
```

... continues on next page ...

. . . continued from previous page . . .

```
http://www.seclab.net/dav/puttest647009096.html
```

Impact

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

Solution:

Solution type: Mitigation

Use access restrictions to these dangerous HTTP methods or disable them completely.

Affected Software/OS

Web servers with enabled PUT and/or DELETE methods.

Vulnerability Detection Method

Checks if dangerous HTTP methods such as PUT and DELETE are enabled and can be misused to upload or delete files.

Details: `Test HTTP dangerous methods`

OID:1.3.6.1.4.1.25623.1.0.10498

Version used: `2022-05-12T09:32:01Z`

References

```
url: http://www.securityfocus.com/bid/12141
owasp: OWASP-CM-001
```

High (CVSS: 7.5)

NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Summary

PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result

```
By doing the following HTTP POST request:
"HTTP POST" body : <?php phpinfo();?>
URL              : http://www.seclab.net/cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%7
↪5%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D
↪%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%
↪6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+
↪%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%
↪72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%6
↪3%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E
↪%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E
it was possible to execute the "<?php phpinfo();?>" command.
Result: <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NO
```

. . . continues on next page . . .

... continued from previous page ...

```
↪ARCHIVE" /></head>
```

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

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

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

Vulnerability Detection Method
Sends a crafted HTTP POST request and checks the response.
Details: `PHP-CGI-based setups vulnerability when parsing query string parameters from ph.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2012-1823
cve: CVE-2012-2311
cve: CVE-2012-2336
cve: CVE-2012-2335
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-ri
↪sks-Update-1567532.html
url: http://www.kb.cert.org/vuls/id/520827
url: http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
url: https://bugs.php.net/bug.php?id=61910
url: http://www.php.net/manual/en/security.cgi-bin.php
url: http://www.securityfocus.com/bid/53388
dfn-cert: DFN-CERT-2013-1494
dfn-cert: DFN-CERT-2012-1316
dfn-cert: DFN-CERT-2012-1276
dfn-cert: DFN-CERT-2012-1268
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-1267
dfn-cert: DFN-CERT-2012-1266
dfn-cert: DFN-CERT-2012-1173
dfn-cert: DFN-CERT-2012-1101
dfn-cert: DFN-CERT-2012-0994
dfn-cert: DFN-CERT-2012-0993
dfn-cert: DFN-CERT-2012-0992
dfn-cert: DFN-CERT-2012-0920
dfn-cert: DFN-CERT-2012-0915
dfn-cert: DFN-CERT-2012-0914
dfn-cert: DFN-CERT-2012-0913
dfn-cert: DFN-CERT-2012-0907
dfn-cert: DFN-CERT-2012-0906
dfn-cert: DFN-CERT-2012-0900
dfn-cert: DFN-CERT-2012-0880
dfn-cert: DFN-CERT-2012-0878
```

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

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

Vulnerability Detection Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://www.seclab.net/mutillidae/phpinfo.php
http://www.seclab.net/phpinfo.php
```

Impact
Some of the information that can be gathered from this file includes:
The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

Solution:
Solution type: Workaround
Delete the listed files or restrict access to them.

Vulnerability Detection Method
Details: `phpinfo() output Reporting`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `2020-08-24T15:18:35Z`

[return to 10.200.0.12]

2.1.2 High general/tcp

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

Product detection result

```
cpe:/o:canonical:ubuntu_linux:8.04
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

Summary

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

Vulnerability Detection Result

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

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: `2022-04-05T13:00:52Z`

Product Detection Result

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

[return to 10.200.0.12]

2.1.3 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10

Summary
TWiki is prone to a cross-site request forgery (CSRF) vulnerability.

Vulnerability Detection Result

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

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

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

Affected Software/OS
TWiki version prior to 4.3.2

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

Vulnerability Detection Method
Details: `TWiki Cross-Site Request Forgery Vulnerability - Sep10`
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: `2022-02-18T13:05:59Z`

References

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

Medium (CVSS: 6.1)
NVT: TWiki < 6.1.0 XSS Vulnerability

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

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      6.1.0
```

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

Affected Software/OS
TWiki version 6.0.2 and probably prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `TWiki < 6.1.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141830
Version used: `2021-08-30T08:01:20Z`

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

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

Summary
jQuery is vulnerable to Cross-site Scripting (XSS) attacks.

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

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

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2021-06-11T08:43:18Z`

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-2020-0590
```

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

Summary

TWiki is prone to a cross-site request forgery (CSRF) vulnerability.

Vulnerability Detection Result

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

Impact

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

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

Affected Software/OS

TWiki version prior to 4.3.1

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Method

Details: `TWiki Cross-Site Request Forgery Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: `2022-02-22T15:13:46Z`

References

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

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.

Vulnerability Detection Result

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

Impact

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

Solution:

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

Affected Software/OS

Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight

It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method

Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.11213
Version used: 2022-05-12T09:32:01Z

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: 5.0)
NVT: /doc directory browsable

Summary

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

Vulnerability Detection Result

```
Vulnerable URL: http://www.seclab.net/doc/
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:

Solution type: Mitigation

Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:

<Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory>

Vulnerability Detection Method

Details: `/doc directory browsable`

OID:1.3.6.1.4.1.25623.1.0.10056

Version used: `2022-05-12T09:32:01Z`

References

```
cve: CVE-1999-0678
url: http://www.securityfocus.com/bid/318
```

Medium (CVSS: 5.0)

NVT: QWikiwiki directory traversal vulnerability

Summary

The remote host is running QWikiwiki, a Wiki application written in PHP.

The remote version of this software contains a validation input flaw which may allow an attacker to use it to read arbitrary files on the remote host with the privileges of the web server.

Vulnerability Detection Result

```
Vulnerable URL: http://www.seclab.net/mutillidae/index.php?page=../../../../../.
↪./../../../../../../etc/passwd%00
```

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.

Vulnerability Detection Method

Details: `QWikiwiki directory traversal vulnerability`

OID:1.3.6.1.4.1.25623.1.0.16100

Version used: `2022-05-12T09:32:01Z`

References

```
cve: CVE-2005-0283
url: http://www.securityfocus.com/bid/12163
```

Medium (CVSS: 5.0)
NVT: awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check

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

Vulnerability Detection Result

```
Vulnerable URL: http://www.seclab.net/mutillidae/index.php?page=/etc/passwd
```

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

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

Affected Software/OS
awiki version 20100125 and prior.

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check`
OID:1.3.6.1.4.1.25623.1.0.103210
Version used: `2022-06-08T09:12:49Z`

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

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

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

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://www.seclab.net/dvwa/login.php:password
http://www.seclab.net/phpMyAdmin/:pma_password
http://www.seclab.net/phpMyAdmin/?D=A:pma_password
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://www.seclab.net/tikiwiki/tiki-install.php:pass
http://www.seclab.net/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword
```

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:

Solution type: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

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

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)

- HTTP Forms (e.g. Login) with input field of type 'password'

Details: `Cleartext Transmission of Sensitive Information via HTTP`

OID:1.3.6.1.4.1.25623.1.0.108440

Version used: `2020-08-24T15:18:35Z`

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: jQuery < 1.6.3 XSS Vulnerability

Summary

jQuery is vulnerable to Cross-site Scripting (XSS) attacks.

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability 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: `2021-06-11T09:02:34Z`

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

Product detection result
```
cpe:/a:apache:http_server:2.2.8
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)
```

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

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

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

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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`

Product Detection Result
Product: `cpe:/a:apache:http_server:2.2.8`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

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

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

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

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

Affected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

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

Vulnerability Detection Method
Details: `phpMyAdmin 'error.php' Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: `2022-02-18T13:05:59Z`

References

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-0016
dfn-cert: DFN-CERT-2011-0002
```

[return to 10.200.0.12]

2.1.4 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 612722
Packet 2: 612834
```

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`
OID:1.3.6.1.4.1.25623.1.0.80091

. . . continues on next page . . .

... continued from previous page ...

Version used: 2020-08-24T08:40:10Z

References

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

[return to 10.200.0.12]

This file was automatically generated.