Scan Report

May 9, 2021

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 “ws1”. The scan started at Sat May 8 23:34:34 2021 UTC and ended at Sat May 8 23:44:33 2021 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
192.168.1.176	3	5	1	0	0
Total: 1	3	5	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 9 results selected by the filtering described above. Before filtering there were 221 results.

2 Results per Host

2.1 192.168.1.176

Host scan start	Sat May 8 23:35:00 2021 UTC
Host scan end	Sat May 8 23:44:28 2021 UTC

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

2.1.1 High 80/tcp

High (CVSS: 7.5)
NVT: Basic Analysis and Security Engine Multiple Input Validation Vulnerabilities

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Basic Analysis and Security Engine (BASE) is prone to multiple input-validation vulnerabilities because it fails to adequately sanitize user-supplied input. These vulnerabilities include an SQL-injection issue, a cross-site scripting issue, and a local file-include issue.

Vulnerability Detection Result

```
Installed version: 1.2.6
Fixed version:     1.4.4
```

Impact

Exploiting these issues can allow an attacker to steal cookie-based authentication credentials, view and execute local files within the context of the webserver, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. Other attacks may also be possible.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for details.

Affected Software/OS

These issues affect versions prior to BASE 1.4.4.

Vulnerability Detection Method

Details: `Basic Analysis and Security Engine Multiple Input Validation Vulnerabilities`

OID:1.3.6.1.4.1.25623.1.0.100323

Version used: `2020-10-20T15:03:35Z`

References

```
cve: CVE-2009-4590
cve: CVE-2009-4591
cve: CVE-2009-4592
cve: CVE-2009-4837
cve: CVE-2009-4838
cve: CVE-2009-4839
bid: 36830
bid: 18298
url: http://www.securityfocus.com/bid/36830
```

[return to 192.168.1.176]

2.1.2 High 22/tcp

High (CVSS: 7.5)
NVT: Deprecated SSH-1 Protocol Detection

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptograhic flaws.

Vulnerability Detection Result

```
The service is providing / accepting the following deprecated versions of the SS
↪H protocol which have known cryptograhic flaws:
1.33
1.5
```

Impact

Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Solution:

Solution type: VendorFix

Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

Affected Software/OS

Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

Vulnerability Detection Method

Details: `Deprecated SSH-1 Protocol Detection`

OID:1.3.6.1.4.1.25623.1.0.801993

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

References

```
cve: CVE-2001-0361
cve: CVE-2001-0572
cve: CVE-2001-1473
bid: 2344
url: http://www.kb.cert.org/vuls/id/684820
url: http://xforce.iss.net/xforce/xfdb/6603
```

[return to 192.168.1.176]

2.1.3 High 55/tcp

High (CVSS: 10.0)
NVT: Possible Backdoor: Ingreslock

Summary

A backdoor is installed on the remote host.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
The service is answering to an 'id;' command with the following response: uid=0(
↪root) gid=0(root)
```

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

Solution:
Solution type: Workaround
A whole cleanup of the infected system is recommended.

Vulnerability Detection Method
Details: `Possible Backdoor: Ingreslock`
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: `2020-08-24T08:40:10Z`

[return to 192.168.1.176]

2.1.4 Medium 80/tcp

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2021-02-15T07:14:40Z`

References

```
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
bid: 9506
bid: 9561
bid: 11604
bid: 15222
bid: 19915
bid: 24456
bid: 33374
bid: 36956
bid: 36990
bid: 37995
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.kb.cert.org/vuls/id/867593
url: 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
```

Medium (CVSS: 5.0)
NVT: Backup File Scanner (HTTP) - Reliable Detection Reporting

Summary

The script reports backup files left on the web server.
Notes:
- ’Reliable Detection’ means that a file was detected based on a strict (regex) and reliable pattern matching the response of the remote web server when a file was requested.

. . . continues on next page . . .

... continued from previous page ...

- As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Result

```
The following backup files were identified (<URL>:<Matching pattern>):
http://192.168.1.176/phpmyadmin/config.inc.php~:^<\?(php|=)
```

Impact

Based on the information provided in this files an attacker might be able to gather sensitive information stored in these files.

Solution:

Solution type: Mitigation

Delete the backup files.

Vulnerability Detection Method

Reports previous enumerated backup files accessible on the remote web server.

Details: `Backup File Scanner (HTTP) - Reliable Detection Reporting`

OID:1.3.6.1.4.1.25623.1.0.108976

Version used: `2021-01-21T10:06:42Z`

References

`url: http://www.openwall.com/lists/oss-security/2017/10/31/1`

Medium (CVSS: 4.3)

NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Product detection result

```
cpe:/a:apache:http_server:1.3.37
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:

Solution type: VendorFix

... continues on next page ...

. . . continued from previous page . . .

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: `2021-02-25T13:36:35Z`

Product Detection Result
Product: `cpe:/a:apache:http_server:1.3.37`
Method: `Apache HTTP Server Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
```
cve: CVE-2012-0053
bid: 51706
url: http://secunia.com/advisories/47779
url: http://www.exploit-db.com/exploits/18442
url: http://rhn.redhat.com/errata/RHSA-2012-0128.html
url: http://httpd.apache.org/security/vulnerabilities_22.html
url: http://svn.apache.org/viewvc?view=revision&revision=1235454
url: http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html
```

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

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

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

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

Solution:
Solution type: WillNotFix

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
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: `2019-12-05T15:10:00Z`

References

```
cve: CVE-2010-4480
url: http://www.exploit-db.com/exploits/15699/
url: http://www.vupen.com/english/advisories/2010/3133
```

[return to 192.168.1.176]

2.1.5 Medium 22/tcp

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

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

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

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

Solution:
Solution type: Mitigation
Disable the weak encryption algorithms.

Vulnerability Insight
The ‘arcfour‘ cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
The ‘none‘ algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details: `SSH Weak Encryption Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2020-08-24T08:40:10Z`

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

[return to 192.168.1.176]

2.1.6 Low 22/tcp

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

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

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
```

Solution:
Solution type: Mitigation
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details: SSH Weak MAC Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2020-08-24T08:40:10Z

[return to 192.168.1.176]