Scan Report

May 25, 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 "kali_juiceShop_active". The scan started at Thu May 20 08:42:02 2021 UTC and ended at Thu May 20 08:52:28 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
127.0.0.1 localhost	0	2	0	38	0
Total: 1	0	2	0	38	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 "High" are not shown.
Issues with the threat level "Medium" are not shown.
Issues with the threat level "Low" are not shown.
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 40 results selected by the filtering described above. Before filtering there were 41 results.

2 Results per Host

2.1 127.0.0.1

Host scan start	Thu May 20 08:42:26 2021 UTC
Host scan end	Thu May 20 08:52:22 2021 UTC

Service (Port)	Threat Level
9392/tcp	Medium
5432/tcp	Medium
9392/tcp	Log
5432/tcp	Log
general/CPE-T	Log
80/tcp	Log
3000/tcp	Log
general/tcp	Log

2.1.1 Medium 9392/tcp

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.

Vulnerability Detection Result
```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (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 containing 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: `2021-03-29T06:11:47Z`

References
```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverab
↪les/algorithms-key-sizes-and-parameters-report
url: https://bettercrypto.org/
```

. . . continues on next page . . .

... continued from previous page ...

```
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
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
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
```

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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
```

[return to 127.0.0.1]

2.1.2 Medium 5432/tcp

Medium (CVSS: 5.0)
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.

Vulnerability Detection Result
`'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:`
`TLS_RSA_WITH_SEED_CBC_SHA`

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2020-11-26T08:02:59Z`

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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-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
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

... continues on next page ...

... continued from previous page ...

```
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
```

[return to 127.0.0.1]

2.1.3 Log 9392/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A TLScustom server answered on this port`

Solution:

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: CN=kali
subject alternative names (SAN):
kali
```

... continues on next page ...

... continued from previous page ...

```
issued by .: CN=kali
serial ....: 7B2EC9F91EC9EF6D2C22F03655E49A4B3A69CCCC
valid from : 2021-02-23 10:22:09 UTC
valid until: 2031-02-21 10:22:09 UTC
fingerprint (SHA-1): 2E5962F6C655D2159634B335A2A8222307B884DE
fingerprint (SHA-256): 0D8785B6ED1124A407128B1FECB743CD99968A5B3890B8A46AAC192E7
↪C11C824
```

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2021-04-16T08:08:22Z

Log (CVSS: 0.0)
NVT: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

Vulnerability Detection Result

```
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
Greenbone Security Assistant
-----
```

Solution:

Vulnerability Insight
This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page, authentication page or redirect instead.
The Scanner might enabled some counter measures for that, however they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT. In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

... continues on next page ...

... continued from previous page ...

Log Method
Details: `Response Time / No 404 Error Code Check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `2020-11-27T13:32:50Z`

Log (CVSS: 0.0)
NVT: Greenbone Security Assistant (GSA) Detection

Summary
The script sends a connection request to the server and attempts to determine if it is a GSA from the reply.

Vulnerability Detection Result
```
Detected Greenbone Security Assistant
Version:        unknown
Location:       /
CPE:            cpe:/a:greenbone:greenbone_security_assistant
```

Solution:

Log Method
Details: `Greenbone Security Assistant (GSA) Detection`
OID:1.3.6.1.4.1.25623.1.0.103841
Version used: `2021-04-15T13:23:31Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.
As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead.

Vulnerability Detection Result
```
No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
```

... continues on next page ...

... continued from previous page ...

```
No 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
```

Solution:

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: 2021-01-21T10:06:42Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result

```
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
```

... continues on next page ...

... continued from previous page ...

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2020-03-31T06:57:15Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
```

Solution:

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: 2020-03-31T06:57:15Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Vulnerability Detection Result

```
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
```

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2020-03-31T06:57:15Z

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Summary
The remote web server is not enforcing HSTS.

Vulnerability Detection Result

```
The remote web server is not enforcing HSTS.
HTTP-Banner:
HTTP/1.1 200 OK
Connection: close
Content-Length: ***replaced***
Content-Security-Policy: default-src 'self' 'unsafe-inline'; img-src 'self' blob
↪:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Expires: ***replaced***
Last-Modified: ***replaced***
Date: ***replaced***
```

Solution:
Solution type: Workaround
Enable HSTS or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: 2021-01-26T13:20:44Z

References

```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transpor
↪t_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-securit
↪y-hsts
```

... continues on next page ...

... continued from previous page ...

```
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header
```

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

Summary
The remote web server is not enforcing HPKP.
Note: Most major browsers have dropped / deprecated support for this header in 2020.

Vulnerability Detection Result

```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 200 OK
Connection: close
Content-Length: ***replaced***
Content-Security-Policy: default-src 'self' 'unsafe-inline'; img-src 'self' blob
↪:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Expires: ***replaced***
Last-Modified: ***replaced***
Date: ***replaced***
```

Solution:
Solution type: Workaround
Enable HPKP or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: 2021-01-26T13:20:44Z

References

```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-
```

... continues on next page ...

... continued from previous page ...

```
↪for-http-hpkp
url: https://tools.ietf.org/html/rfc7469
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header
```

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Vulnerability Detection Result

```
Header Name              | Header Value
-------------------------------------------------------------------------------
↪-
Content-Security-Policy | default-src 'self' 'unsafe-inline'; img-src 'self' blo
↪b
X-Frame-Options          | SAMEORIGIN
Missing Headers                    | More Information
-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪----------
Document-Policy                    | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                          | https://owasp.org/www-project-secure-headers
↪/#expect-ct
Feature-Policy                     | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                 | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                    | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                    | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Strict-Transport-Security          | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options             | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
```

... continues on next page ...

... continued from previous page ...

```
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `2021-01-26T13:20:44Z`

References
`url: https://owasp.org/www-project-secure-headers/`
`url: https://owasp.org/www-project-secure-headers/#div-headers`
`url: https://securityheaders.io/`

Log (CVSS: 0.0)
NVT: robot(s).txt exists on the Web Server

Summary
Web Servers can use a file called /robot(s).txt to ask search engines to ignore certain files and directories. By nature this file can not be used to protect private files from public read access.

Vulnerability Detection Result

```
The file 'https://localhost:9392/robots.txt' contains the following:
User-agent: *
Disallow: /
```

Solution:
Solution type: Mitigation
Review the content of the /robot(s).txt file and consider removing the files from the server or protect them in other ways in case you actually intended non-public availability.

Vulnerability Insight
Any serious web search engine will honor the /robot(s).txt file and not scan the files and directories listed there.
Any entries listed in this file are not even hidden anymore.

Log Method
Details: `robot(s).txt exists on the Web Server`
OID:1.3.6.1.4.1.25623.1.0.10302
Version used: `2020-08-24T15:18:35Z`

... continues on next page ...

... continued from previous page ...

References

url: https://www.robotstxt.org/
url: https://www.robotstxt.org/norobots-rfc.txt

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "localhost" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
Greenbone Security Assistant
-----
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
https://localhost:9392/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because the "Regex pat
↪tern to exclude directories from CGI scanning" setting of the NVT "Global vari
↪able settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\
```

... continues on next page ...

... continued from previous page ...

↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
https://localhost:9392/img
https://localhost:9392/static/css
https://localhost:9392/static/js

Solution:

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2020-11-19T14:17:11Z

References
url: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A web server is running on this port through SSL

Solution:

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2021-03-15T10:42:03Z

[return to 127.0.0.1]

2.1.4 Log 5432/tcp

Log (CVSS: 0.0)
NVT: Services

Summary

... continues on next page ...

... continued from previous page ...

This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`An unknown service is running on this port.`
`It is usually reserved for Postgres`

Solution:

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: PostgreSQL SSL/TLS Support Detection

Product detection result
`cpe:/a:postgresql:postgresql`
`Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)`

Summary
Checks if the remote PostgreSQL server supports SSL/TLS.

Vulnerability Detection Result
`The remote PostgreSQL server supports SSL/TLS.`

Solution:

Log Method
Details: `SSL/TLS: PostgreSQL SSL/TLS Support Detection`
OID:1.3.6.1.4.1.25623.1.0.105013
Version used: `2020-01-28T13:26:39Z`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql`
Method: `PostgreSQL Detection`
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
`url: https://www.postgresql.org/docs/current/static/ssl-tcp.html`

Log (CVSS: 0.0)
NVT: PostgreSQL Detection

Summary
Detection of PostgreSQL, an open source object-relational database system.
The script sends a connection request to the server (user:postgres, DB:postgres) and attempts to extract the version number from the reply.

Vulnerability Detection Result
```
Detected PostgreSQL
Version:       unknown
Location:      5432/tcp
CPE:           cpe:/a:postgresql:postgresql
Concluded from version/product identification result:
0x00:  52 00 00 00 0C 00 00 00 05 B2 9D 72 7D             R..........r}
```

Solution:

Log Method
Details: `PostgreSQL Detection`
OID:1.3.6.1.4.1.25623.1.0.100151
Version used: `2020-11-12T10:09:08Z`

References
`url: https://www.postgresql.org/`

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result
```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: CN=kali
subject alternative names (SAN):
kali
issued by .: CN=kali
serial ....: 7B2EC9F91EC9EF6D2C22F03655E49A4B3A69CCCC
valid from : 2021-02-23 10:22:09 UTC
valid until: 2031-02-21 10:22:09 UTC
fingerprint (SHA-1): 2E5962F6C655D2159634B335A2A8222307B884DE
fingerprint (SHA-256): 0D8785B6ED1124A407128B1FECB743CD99968A5B3890B8A46AAC192E7
↪C11C824
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2021-04-16T08:08:22Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Self-Signed Certificate Detection

Summary
The SSL/TLS certificate on this port is self-signed.

Vulnerability Detection Result
```
The certificate of the remote service is self signed.
Certificate details:
subject ...: CN=kali
subject alternative names (SAN):
kali
issued by .: CN=kali
serial ....: 7B2EC9F91EC9EF6D2C22F03655E49A4B3A69CCCC
valid from : 2021-02-23 10:22:09 UTC
valid until: 2031-02-21 10:22:09 UTC
fingerprint (SHA-1): 2E5962F6C655D2159634B335A2A8222307B884DE
fingerprint (SHA-256): 0D8785B6ED1124A407128B1FECB743CD99968A5B3890B8A46AAC192E7
↪C11C824
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: 2018-02-28T12:15:33Z

References
url: http://en.wikipedia.org/wiki/Self-signed_certificate

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.

... continues on next page ...

... continued from previous page ...

As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead.

Vulnerability Detection Result

'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
```

Solution:

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: 2021-01-21T10:06:42Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result

```
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
```

... continues on next page ...

... continued from previous page ...

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2020-03-31T06:57:15Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CCM

... continues on next page ...

... continued from previous page ...

TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256

Solution:

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: 2020-03-31T06:57:15Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Vulnerability Detection Result
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_DHE_RSA_WITH_SEED_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2020-03-31T06:57:15Z

[return to 127.0.0.1]

2.1.5 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan. Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

Vulnerability Detection Result
`127.0.0.1|cpe:/a:greenbone:greenbone_security_assistant`
`127.0.0.1|cpe:/a:jquery:jquery`
`127.0.0.1|cpe:/a:postgresql:postgresql`
`127.0.0.1|cpe:/o:linux:kernel`

Solution:
Log Method Details: `CPE Inventory` OID:1.3.6.1.4.1.25623.1.0.810002 Version used: `2021-04-16T10:39:13Z`
References `url: https://nvd.nist.gov/products/cpe`

[return to 127.0.0.1]

2.1.6 Log 80/tcp

Log (CVSS: 0.0) NVT: Services
Summary This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Vulnerability Detection Result `A web server is running on this port`
Solution:
. . . continues on next page . . .

... continued from previous page ...

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2021-03-15T10:42:03Z

Log (CVSS: 0.0)
NVT: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

Vulnerability Detection Result
The host returns a 30x (e.g. 301) error code when a non-existent file is request
↪ed. Some HTTP-related checks have been disabled.

Solution:

Vulnerability Insight
This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page, authentication page or redirect instead.
The Scanner might enabled some counter measures for that, however they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT. In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

Log Method
Details: Response Time / No 404 Error Code Check
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: 2020-11-27T13:32:50Z

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.

... continues on next page ...

... continued from previous page ...

This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "localhost" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://localhost/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method

Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2020-11-19T14:17:11Z

References

url: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary

All known security headers are being checked on the remote web server.

... continues on next page ...

... continued from previous page ...

On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Vulnerability Detection Result

```
Header Name             | Header Value
------------------------------------------------------------------------------
↪-
Content-Security-Policy | default-src 'self' 'unsafe-inline'; img-src 'self' blo
↪b
X-Frame-Options         | SAMEORIGIN
Missing Headers                   | More Information
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-------------------------
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method

Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-01-26T13:20:44Z

References

url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.io/

[return to 127.0.0.1]

2.1.7 Log 3000/tcp

Log (CVSS: 0.0)
NVT: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

Vulnerability Detection Result
```
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
OWASP Juice Shop
-----
```

Solution:

Vulnerability Insight
This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page, authentication page or redirect instead.
The Scanner might enabled some counter measures for that, however they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT. In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

Log Method
Details: `Response Time / No 404 Error Code Check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `2020-11-27T13:32:50Z`

Log (CVSS: 0.0)
NVT: jQuery Detection (HTTP)

Summary
HTTP based detection of jQuery.

Vulnerability Detection Result
```
Detected jQuery
Version:        unknown
Location:       Externally hosted
CPE:            cpe:/a:jquery:jquery
```

. . . continues on next page . . .

... continued from previous page ...

```
Concluded from version/product identification result:
src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js embedded into U
↪RL /
Extra information:
The jQuery library is hosted on a different server. Because of this it is not po
↪ssible to gather the version by a direct file access. Please manually inspect
↪the version which gets included on this web page.
```

Solution:

Log Method
Details: jQuery Detection (HTTP)
OID:1.3.6.1.4.1.25623.1.0.141622
Version used: 2021-05-17T10:34:03Z

References
url: https://jquery.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Vulnerability Detection Result

```
Header Name             | Header Value
----------------------------------------
Feature-Policy          | payment 'self'
X-Content-Type-Options  | nosniff
X-Frame-Options         | SAMEORIGIN
Missing Headers                     | More Information
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪--------------------------
Content-Security-Policy             | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Document-Policy                     | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Permissions-Policy                  | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                     | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
```

... continues on next page ...

... continued from previous page ...

X-XSS-Protection	https://owasp.org/www-project-secure-headers/#x-xss-protection, Note: Most major browsers have dropped / deprecated support for this header in 2020.

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-01-26T13:20:44Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.io/

Log (CVSS: 0.0)
NVT: robot(s).txt exists on the Web Server

Summary
Web Servers can use a file called /robot(s).txt to ask search engines to ignore certain files and directories. By nature this file can not be used to protect private files from public read access.

Vulnerability Detection Result
The file 'http://localhost:3000/robots.txt' contains the following:
User-agent: *
Disallow: /ftp

Solution:
Solution type: Mitigation
Review the content of the /robot(s).txt file and consider removing the files from the server or protect them in other ways in case you actually intended non-public availability.

Vulnerability Insight
Any serious web search engine will honor the /robot(s).txt file and not scan the files and directories listed there.
Any entries listed in this file are not even hidden anymore.

Log Method
Details: robot(s).txt exists on the Web Server
OID:1.3.6.1.4.1.25623.1.0.10302
Version used: 2020-08-24T15:18:35Z

References

... continues on next page ...

... continued from previous page ...

```
url: https://www.robotstxt.org/
url: https://www.robotstxt.org/norobots-rfc.txt
```

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "localhost" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
The service is responding with a 200 HTTP status code to non-existent files/urls
↪. The following pattern is used to work around possible false detections:
-----
OWASP Juice Shop
-----
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://localhost:3000/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: `CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2020-11-19T14:17:11Z`

References
`url: https://community.greenbone.net/c/vulnerability-tests`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A web server is running on this port`

Solution:

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2021-03-15T10:42:03Z`

[return to 127.0.0.1]

2.1.8 Log general/tcp

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Vulnerability Detection Result
```
The following additional and resolvable hostnames pointing to a different host i
↪p were detected:
kali
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: 2020-11-10T15:30:28Z

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several VTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result

```
Best matching OS:
OS:            Linux/Unix
CPE:           cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.103841 (Greenbone Security Assistant (GSA) D
↪etection)
Setting key "Host/runs_unixoide" based on this information
```

Solution:

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2021-05-17T10:34:03Z

References
url: https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Network route from scanner (127.0.0.1) to target (127.0.0.1):
127.0.0.1
Network distance between scanner and target: 1
```

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `2021-03-12T14:25:59Z`

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Vulnerability Detection Result

```
Hostname determination for IP 127.0.0.1:
Hostname|Source
localhost|Reverse-DNS
```

Solution:

Log Method
Details: `Hostname Determination Reporting`
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: `2018-11-19T11:11:31Z`

[return to 127.0.0.1]