Scan Report

August 1, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP app.offision.com". The scan started at Thu Aug 1 03:49:17 2024 UTC and ended at Thu Aug 1 04:43:59 2024 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
20.43.67.39 app.offision.com	0	0	1	26	0
Total: 1	0	0	1	26	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 "Debug" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 27 results selected by the filtering described above. Before filtering there were 30 results.

2 Results per Host

2.1 20.43.67.39

Host scan start	Thu Aug 1 03:50:07 2024 UTC
Host scan end	Thu Aug 1 04:43:56 2024 UTC

Service (Port)	Threat Level
general/tcp	Low
443/tcp	Log
general/CPE-T	Log
general/tcp	Log

2.1.1 Low general/tcp

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1229211950
Packet 2: 1229213320
```

Impact

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

Solution:

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight

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

Vulnerability Detection Method

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

Details: `TCP Timestamps Information Disclosure`

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: `2023-12-15T16:10:08Z`

References

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

[return to 20.43.67.39]

2.1.2 Log 443/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
A web server is running on this port through SSL
```

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
TLSv1.2
TLSv1.3
```

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2024-07-24T05:06:37Z

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.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | C47EF8BF9DF21719DED4DC15408C07F69CBDCAF3
fingerprint (SHA-256)           | 7777C4BEFAA2806813E846D40E834CCED83F2593886AAC
↪05E64E11199D341A81
issued by                       | CN=Microsoft Azure RSA TLS Issuing CA 04,O=Mic
↪rosoft Corporation,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 330051E1512B7DDC1FA0A67AA200000051E151
signature algorithm             | sha384WithRSAEncryption
subject                         | CN=*.azurewebsites.net,O=Microsoft Corporation
↪,L=Redmond,ST=WA,C=US
subject alternative names (SAN) | *.sso.japaneast-01.azurewebsites.net, *.japane
↪ast.c.azurewebsites.net, *.scm.japaneast.c.azurewebsites.net, *.sso.japaneast.
↪c.azurewebsites.net, *.azure-mobile.net, *.scm.azure-mobile.net, *.azurewebsit
↪es.net, *.scm.azurewebsites.net, *.sso.azurewebsites.net, *.japaneast-01.azure
↪websites.net, *.scm.japaneast-01.azurewebsites.net
valid from                      | 2024-05-24 15:17:41 UTC
valid until                     | 2025-05-19 15:17:41 UTC
```

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-06-14T05:05:48Z

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner   | Enumeration technique
---------------------------------------------------------------------------
Server: Kestrel | Valid HTTP 1.1 GET request (with extended headers) to '/'
```

Solution:

Log Method

Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2022-06-28T10:11:01Z`

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.

Quality of Detection (QoD): 80%

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:
-----
404
-----
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2023-07-07T05:05:26Z`

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Header Name               | Header Value
-------------------------------------------------
Content-Security-Policy   | frame-ancestors https
Strict-Transport-Security | max-age=2592000
X-Frame-Options           | SAMEORIGIN
Missing Headers                   | More Information
--------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪----------
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
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, Note: This is an upcoming 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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
Sec-Fetch-Dest                     | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                     | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                     | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                     | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
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: 2021-07-14T06:19:43Z

References

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

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

Product detection result

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

. . . continues on next page . . .

. . . continued from previous page . . .

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
'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_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_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
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_GCM_SHA384
'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_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: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "app.offision.com".
Certificate details:
fingerprint (SHA-1)             | C47EF8BF9DF21719DED4DC15408C07F69CBDCAF3
fingerprint (SHA-256)           | 7777C4BEFAA2806813E846D40E834CCED83F2593886AAC
↪05E64E11199D341A81
issued by                       | CN=Microsoft Azure RSA TLS Issuing CA 04,O=Mic
↪rosoft Corporation,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 330051E1512B7DDC1FA0A67AA200000051E151
signature algorithm             | sha384WithRSAEncryption
subject                         | CN=*.azurewebsites.net,O=Microsoft Corporation
↪,L=Redmond,ST=WA,C=US
subject alternative names (SAN) | *.sso.japaneast-01.azurewebsites.net, *.japane
↪ast.c.azurewebsites.net, *.scm.japaneast.c.azurewebsites.net, *.sso.japaneast.
↪c.azurewebsites.net, *.azure-mobile.net, *.scm.azure-mobile.net, *.azurewebsit
↪es.net, *.scm.azurewebsites.net, *.sso.azurewebsites.net, *.japaneast-01.azure
↪websites.net, *.scm.japaneast-01.azurewebsites.net
valid from                      | 2024-05-24 15:17:41 UTC
valid until                     | 2025-05-19 15:17:41 UTC
```

Solution:

Log Method

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if the remote web server has HTTP Strict Transport Security (HSTS) enabled.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote web server is sending the "HTTP Strict-Transport-Security" header.
HSTS-Header:
Strict-Transport-Security: max-age=2592000
```

Solution:

Log Method

Details: `SSL/TLS: HTTP Strict Transport Security (HSTS) Detection`
OID:1.3.6.1.4.1.25623.1.0.105876
Version used: `2024-02-08T05:05:59Z`

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
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: SSL/TLS: Check for ‘max-age‘ Attribute in HSTS Header

Summary

The remote web server is using a too low value within the ’max-age’ attribute in the HTTP Strict Transport Security (HSTS) header.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote web server is using a value of "2592000" within the "max-age" attribu
↪te in the HSTS header. This value is below the configured / minimal recommende
↪d value of "10886400".
HSTS Header:
Strict-Transport-Security: max-age=2592000
```

Solution:

Solution type: Workaround

The minimum value to get added to the HSTS preload lists of Google Chrome is 18 weeks (10886400 seconds). The value should aim towards 6 months (15768000 seconds) but heavily depends on your deployment scenario.

. . . continues on next page . . .

. . . continued from previous page . . .

Log Method
Details: SSL/TLS: Check for ‘max-age‘ Attribute in HSTS Header
OID:1.3.6.1.4.1.25623.1.0.108251
Version used: 2024-02-08T05:05:59Z

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
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
```

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

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 200 OK
Content-Length: ***replaced***
Connection: close
Content-Type: text/html
Date: ***replaced***
Server: Kestrel
Accept-Ranges: bytes
Cache-Control: max-age=0
ETag: "***replaced***"
Last-Modified: ***replaced***
Strict-Transport-Security: max-age=2592000
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors https://teams.microsoft.com https://off
↪ice.com https://*.office.com https://office365.com https://*.office365.com htt
↪ps://microsoft365.com https://*.microsoft365.com
```

Solution:
Solution type: Workaround

. . . continues on next page . . .

. . . continued from previous page . . .

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: 2024-02-08T05:05:59Z

References

```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-
↪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: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

Summary

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
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_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
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
```

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

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

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

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

Summary

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
'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_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_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
TLS_RSA_WITH_AES_256_GCM_SHA384
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_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: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Report Supported Cipher Suites`
OID: 1.3.6.1.4.1.25623.1.0.802067)

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

Summary

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

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.
'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_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_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
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_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.
'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
TLS_AES_256_GCM_SHA384
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.
```

Solution:

Vulnerability Insight

Notes:

- 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.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method

Details: SSL/TLS: Report Supported Cipher Suites

OID:1.3.6.1.4.1.25623.1.0.802067

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

Log (CVSS: 0.0)
NVT: SSL/TLS: Safe/Secure Renegotiation Support Status

Summary

Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
Protocol Version | Safe/Secure Renegotiation Support Status
--------------------------------------------------------------------------------
↪--------------------------------------------------------------------------------
↪------------------------------------
SSLv3            | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.0          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.1          | Unknown, Reason: Scanner failed to negotiate an SSL/TLS conne
↪ction (Either the scanner or the remote host is probably not supporting / acce
↪pting this SSL/TLS protocol version).
TLSv1.2          | Enabled, Note: While the remote service announces the support
↪ of safe/secure renegotiation it still might not support / accept renegotiatio
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪n at all.
TLSv1.3         | Disabled (The TLSv1.3 protocol generally doesn't support rene
↪gotiation so this is always reported as 'Disabled')
```

Solution:

Log Method
Details: SSL/TLS: Safe/Secure Renegotiation Support Status
OID:1.3.6.1.4.1.25623.1.0.117757
Version used: 2024-07-24T05:06:37Z

References
url: https://www.gnutls.org/manual/html_node/Safe-renegotiation.html
url: https://wiki.openssl.org/index.php/TLS1.3#Renegotiation
url: https://datatracker.ietf.org/doc/html/rfc5746

Log (CVSS: 0.0)
NVT: SSL/TLS: ‘includeSubDomains‘ Missing in HSTS Header

Summary
The remote web server is missing the 'includeSubDomains' attribute in the HTTP Strict Transport Security (HSTS) header.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote web server is missing the "includeSubDomains" attribute in the HSTS h
↪eader.
HSTS Header:
Strict-Transport-Security: max-age=2592000
```

Solution:
Solution type: Workaround
Add the 'includeSubDomains' attribute to the HSTS header.

Log Method
Details: SSL/TLS: ‘includeSubDomains‘ Missing in HSTS Header
OID:1.3.6.1.4.1.25623.1.0.105877
Version used: 2024-02-08T05:05:59Z

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-securit
↪y-hsts
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: SSL/TLS: ‘preload‘ Missing in HSTS Header

Summary
The remote web server is missing the ’preload’ attribute in the HTTP Strict Transport Security (HSTS) header.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote web server is missing the "preload" attribute in the HSTS header.
HSTS Header:
Strict-Transport-Security: max-age=2592000
```

Solution:
Solution type: Workaround
Submit the domain to the ’HSTS preload list’ and add the ’preload’ attribute to the HSTS header.

Log Method
Details: `SSL/TLS: ‘preload‘ Missing in HSTS Header`
OID:1.3.6.1.4.1.25623.1.0.105878
Version used: `2024-02-08T05:05:59Z`

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
url: https://tools.ietf.org/html/rfc6797
url: https://hstspreload.appspot.com/
url: https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: Kestrel
```

Solution:

Log Method

Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary

This routine identifies services supporting the following extensions to TLS:
- Application-Layer Protocol Negotiation (ALPN)
- Next Protocol Negotiation (NPN).

Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote service advertises support for the following Network Protocol(s) via
↪the ALPN extension:
SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1
```

Solution:

Log Method

Details: `SSL/TLS: NPN / ALPN Extension and Protocol Support Detection`
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: `2023-04-18T10:19:20Z`

References

```
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04
```

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
The script consolidates and reports various information for web application (formerly called '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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The Hostname/IP "app.offision.com" 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:
-----
404
-----
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 23.0.1)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://app.offision.com/
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 web application scanning because th
↪e "Regex pattern to exclude directories from CGI scanning" setting of the VT "
↪Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was
↪: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graph
↪ic|grafik|picture|bilder|thumbnail|media/|skins?/)"
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
https://app.offision.com/assets/images
https://app.offision.com/assets/images/device-icon/Assets.xcassets/AppIcon.appic
↪onset/_
https://app.offision.com/assets/images/splash_screens
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-07-03T06:48:05Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
A TLScustom server answered on this port
```

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). 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.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

[return to 20.43.67.39]

2.1.3 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
20.43.67.39|cpe:/a:ietf:transport_layer_security:1.2
20.43.67.39|cpe:/a:ietf:transport_layer_security:1.3
```

Solution:

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2022-07-27T10:11:28Z`

References
url: `https://nvd.nist.gov/products/cpe`

[return to 20.43.67.39]

2.1.4 Log general/tcp

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 forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
No Best matching OS identified. Please see the VT 'Unknown OS and Service Banner
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪ Reporting' (OID: 1.3.6.1.4.1.25623.1.0.108441) for possible ways to identify
↪this OS.
```

Solution:

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2024-07-30T05:05:46Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This VT consolidates and reports the information collected by the following VTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

If you know any of the information reported here, please send the full output to the referenced community forum.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to https://forum.greenbone.net/c/vulnerabili
↪ty-tests/7:
Banner: Server: Kestrel
Identified from: HTTP Server banner on port 443/tcp
```

Solution:

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2023-06-22T10:34:15Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Traceroute

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Network route from scanner (172.20.0.7) to target (20.43.67.39):
172.20.0.7
20.43.67.39
Network distance between scanner and target: 2
```

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: `2022-10-17T11:13:19Z`

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Hostname determination for IP 20.43.67.39:
Hostname|Source
app.offision.com|Forward-DNS
```

Solution:

Log Method
Details: `Hostname Determination Reporting`

... continues on next page ...

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.108449 Version used: `2022-07-27T10:11:28Z`

[return to 20.43.67.39]

This file was automatically generated.