Scan Report

March 8, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "6408c8cefff3836c1950f8fe-6408c8cefff3836c1950f920-4f3489de". The scan started at Wed Mar 8 17:41:56 2023 UTC and ended at Wed Mar 8 19:24:27 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
93.11.145.199	0	0	1	51	0
Total: 1	0	0	1	51	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.
Only results with a minimum QoD of 70 are shown.

This report contains all 52 results selected by the filtering described above. Before filtering there were 53 results.

2 Results per Host

2.1 93.11.145.199

Host scan start	Wed Mar 8 17:42:41 2023 UTC
Host scan end	Wed Mar 8 19:24:22 2023 UTC

Service (Port)	Threat Level
general/tcp	Low
general/CPE-T	Log
5001/tcp	Log
80/tcp	Log
443/tcp	Log
general/tcp	Log
5000/tcp	Log

2.1.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

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

. . . continues on next page . . .

... continued from previous page ...

```
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1952966089
Packet 2: 1952967224
```

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

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

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

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

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

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

[return to 93.11.145.199]

2.1.2 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary

... continues on next page ...

... continued from previous page ...

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
93.11.145.199|cpe:/a:f5:nginx
93.11.145.199|cpe:/a:nginx:nginx
93.11.145.199|cpe:/a:synology:diskstation_manager:7.1.1-42962
93.11.145.199|cpe:/h:synology:unknown_model
93.11.145.199|cpe:/o:synology:unknown_model_firmware:7.1.1-42962

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 93.11.145.199]

2.1.3 Log 5001/tcp

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 forum.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
The Hostname/IP "93.11.145.199" 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 NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)" 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://93.11.145.199:5001/
https://93.11.145.199:5001/oauth
https://93.11.145.199:5001/scripts
https://93.11.145.199:5001/scripts/babel-polyfill
https://93.11.145.199:5001/scripts/ext-3
https://93.11.145.199:5001/scripts/ext-3/adapter/ext
https://93.11.145.199:5001/scripts/ext-3/ux
https://93.11.145.199:5001/scripts/noise
https://93.11.145.199:5001/scripts/scrollbar
https://93.11.145.199:5001/scripts/syno-vue-components
https://93.11.145.199:5001/scripts/synocredential.js
https://93.11.145.199:5001/scripts/synowebapi.js
https://93.11.145.199:5001/scripts/vue
https://93.11.145.199:5001/scripts/vue-router
https://93.11.145.199:5001/scripts/vuex
https://93.11.145.199:5001/synoSDSjslib
https://93.11.145.199:5001/synohdpack
https://93.11.145.199:5001/webapi
https://93.11.145.199:5001/webman
https://93.11.145.199:5001/webman/3rdparty
https://93.11.145.199:5001/webman/3rdparty/ActiveBackup
https://93.11.145.199:5001/webman/3rdparty/ActiveBackup-Portal
https://93.11.145.199:5001/webman/3rdparty/ActiveInsight
https://93.11.145.199:5001/webman/3rdparty/Docker
https://93.11.145.199:5001/webman/3rdparty/FileBrowser
https://93.11.145.199:5001/webman/3rdparty/FileTaskMonitor
https://93.11.145.199:5001/webman/3rdparty/HybridShare
https://93.11.145.199:5001/webman/3rdparty/HyperBackup
https://93.11.145.199:5001/webman/3rdparty/OAuthService
https://93.11.145.199:5001/webman/3rdparty/ScsiTarget
https://93.11.145.199:5001/webman/3rdparty/SynoFinder
https://93.11.145.199:5001/webman/3rdparty/VPNCenter
https://93.11.145.199:5001/webman/3rdparty/Virtualization
```

... continues on next page ...

... continued from previous page ...

https://93.11.145.199:5001/webman/3rdparty/WebStation
https://93.11.145.199:5001/webman/desktop/dist
https://93.11.145.199:5001/webman/entry/dist
https://93.11.145.199:5001/webman/login/dist
https://93.11.145.199:5001/webman/modules
https://93.11.145.199:5001/webman/modules/ActiveInsightUpdateNotify
https://93.11.145.199:5001/webman/modules/AdminCenter
https://93.11.145.199:5001/webman/modules/AudioPlayer
https://93.11.145.199:5001/webman/modules/BackgroundTaskMonitor
https://93.11.145.199:5001/webman/modules/BandwidthControl
https://93.11.145.199:5001/webman/modules/C3
https://93.11.145.199:5001/webman/modules/ClipBoardJS
https://93.11.145.199:5001/webman/modules/ConfigBackup
https://93.11.145.199:5001/webman/modules/DSMNotify
https://93.11.145.199:5001/webman/modules/DataDrivenDocuments
https://93.11.145.199:5001/webman/modules/DesktopProgress
https://93.11.145.199:5001/webman/modules/DisableAdminNotification
https://93.11.145.199:5001/webman/modules/DiskMessageHandler
https://93.11.145.199:5001/webman/modules/EnableNewUpdateSetting
https://93.11.145.199:5001/webman/modules/ExternalDevices
https://93.11.145.199:5001/webman/modules/FileChooser
https://93.11.145.199:5001/webman/modules/FileChooserV6
https://93.11.145.199:5001/webman/modules/HelpBrowser
https://93.11.145.199:5001/webman/modules/HotkeyManager
https://93.11.145.199:5001/webman/modules/LogCenter
https://93.11.145.199:5001/webman/modules/MyDSCenter
https://93.11.145.199:5001/webman/modules/OTPWizard
https://93.11.145.199:5001/webman/modules/PersonalSettings
https://93.11.145.199:5001/webman/modules/PhotoViewer
https://93.11.145.199:5001/webman/modules/PkgManApp
https://93.11.145.199:5001/webman/modules/PollingTask
https://93.11.145.199:5001/webman/modules/ResetAdminApp
https://93.11.145.199:5001/webman/modules/ResourceMonitor
https://93.11.145.199:5001/webman/modules/SecurityScan
https://93.11.145.199:5001/webman/modules/Share
https://93.11.145.199:5001/webman/modules/SharingManager
https://93.11.145.199:5001/webman/modules/StorageManager
https://93.11.145.199:5001/webman/modules/SupportForm
https://93.11.145.199:5001/webman/modules/SystemInfoApp
https://93.11.145.199:5001/webman/modules/TaskSchedulerUtils
https://93.11.145.199:5001/webman/modules/TaskSchedulerWidget
https://93.11.145.199:5001/webman/modules/TinyMCE
https://93.11.145.199:5001/webman/modules/UpdateMaskApp
https://93.11.145.199:5001/webman/modules/Utils
https://93.11.145.199:5001/webman/modules/VideoPlayer2
https://93.11.145.199:5001/webman/modules/WelcomeApp
https://93.11.145.199:5001/webman/modules/Widgets

... continues on next page ...

... continued from previous page ...

```
https://93.11.145.199:5001/webman/resources
https://93.11.145.199:5001/webman/sds/dist
https://93.11.145.199:5001/webman/taskbar/dist
https://93.11.145.199:5001/webman/unsupported-browsers/dist
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\
↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
https://93.11.145.199:5001/scripts/ext-3.4/resources/css
https://93.11.145.199:5001/scripts/syno-vue-components/style
https://93.11.145.199:5001/webman/resources/css
https://93.11.145.199:5001/webman/resources/images
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
https://93.11.145.199:5001/webapi/entry.cgi (method [getjs] version [1] api [SYN
↪O.Core.Desktop.SessionData] SynoToken [] lang [enu] v [1656670912] )
https://93.11.145.199:5001/webman/favicon.ico (v [40438] )
https://93.11.145.199:5001/webman/resources/images/icon_dsm_16.png (v [40438] )
https://93.11.145.199:5001/webman/resources/images/icon_dsm_32.png (v [40438] )
https://93.11.145.199:5001/webman/resources/images/icon_dsm_48.png (v [40438] )
https://93.11.145.199:5001/webman/resources/images/icon_dsm_64.png (v [40438] )
https://93.11.145.199:5001/webman/resources/images/icon_dsm_96.png (v [40438] )
The following cgi scripts were excluded from CGI scanning because of the "Regex
↪pattern to exclude cgi scripts" setting of the NVT "Web mirroring" (OID: 1.3.6
↪.1.4.1.25623.1.0.10662) for this scan was: "\.(js|css)$"
Syntax : cginame (arguments [default value])
https://93.11.145.199:5001/scripts/babel-polyfill/polyfill.js (v [1650348555] )
https://93.11.145.199:5001/scripts/ext-3.4/resources/css/ext-all.css (v [1650348
↪555] )
https://93.11.145.199:5001/scripts/ext-3/adapter/ext/ext-base.js (v [1650348555]
↪ )
https://93.11.145.199:5001/scripts/ext-3/ext-all.js (v [1650348555] )
https://93.11.145.199:5001/scripts/ext-3/ux/ux-all.css (v [1650348555] )
https://93.11.145.199:5001/scripts/ext-3/ux/ux-all.js (v [1650348555] )
https://93.11.145.199:5001/scripts/noise/constants.js (v [1650348555] )
https://93.11.145.199:5001/scripts/noise/index.js (v [1650348555] )
https://93.11.145.199:5001/scripts/noise/noise-c.js (v [1650348555] )
https://93.11.145.199:5001/scripts/noise/sodium.js (v [1650348555] )
https://93.11.145.199:5001/scripts/scrollbar/flexcroll.css (v [1650348555] )
https://93.11.145.199:5001/scripts/scrollbar/flexcroll.js (v [1650348555] )
https://93.11.145.199:5001/scripts/syno-vue-components/style/syno-vue-components
↪.css (v [1652869476] )
https://93.11.145.199:5001/scripts/syno-vue-components/syno-vue-components.min.j
```

... continues on next page ...

... continued from previous page ...

```
↪s (v [1652869476] )
https://93.11.145.199:5001/scripts/synocredential.js/synocredential.min.js (v [1
↪661507553] )
https://93.11.145.199:5001/scripts/synowebapi.js/synowebapi.min.js (v [165328791
↪2] )
https://93.11.145.199:5001/scripts/vue-router/vue-router.min.js (v [1648175353]
↪)
https://93.11.145.199:5001/scripts/vue/vue.min.js (v [1633587521] )
https://93.11.145.199:5001/scripts/vuex/vuex.min.js (v [1585722123] )
https://93.11.145.199:5001/synoSDSjslib/sds.css (v [1654081517] )
https://93.11.145.199:5001/synoSDSjslib/sds.js (v [1654081517] )
https://93.11.145.199:5001/synoSDSjslib/vendor.js (v [1654081517] )
https://93.11.145.199:5001/webman/3rdparty/ActiveBackup-Portal/style.css (v [167
↪1607363] )
https://93.11.145.199:5001/webman/3rdparty/ActiveBackup/style.css (v [1671607373
↪] )
https://93.11.145.199:5001/webman/3rdparty/ActiveInsight/style.css (v [166082676
↪4] )
https://93.11.145.199:5001/webman/3rdparty/Docker/style.css (v [1658399307] )
https://93.11.145.199:5001/webman/3rdparty/FileBrowser/style.css (v [1657097204]
↪ )
https://93.11.145.199:5001/webman/3rdparty/FileTaskMonitor/style.css (v [1657097
↪197] )
https://93.11.145.199:5001/webman/3rdparty/HybridShare/style.css (v [1669297024]
↪ )
https://93.11.145.199:5001/webman/3rdparty/HyperBackup/style.css (v [1666887595]
↪ )
https://93.11.145.199:5001/webman/3rdparty/OAuthService/style.css (v [1618330426
↪] )
https://93.11.145.199:5001/webman/3rdparty/ScsiTarget/style.css (v [1659958512]
↪)
https://93.11.145.199:5001/webman/3rdparty/SynoFinder/style.css (v [1642065031]
↪)
https://93.11.145.199:5001/webman/3rdparty/VPNCenter/style.css (v [1656648365] )
https://93.11.145.199:5001/webman/3rdparty/Virtualization/style.css (v [16618384
↪27] )
https://93.11.145.199:5001/webman/3rdparty/WebStation/style.css (v [1648710000]
↪)
https://93.11.145.199:5001/webman/desktop/dist/dsm.desktop.bundle.js (v [1661421
↪011] )
https://93.11.145.199:5001/webman/desktop/dist/style.css (v [1661421011] )
https://93.11.145.199:5001/webman/entry/dist/dsm.entry.bundle.js (v [1661421011]
↪ )
https://93.11.145.199:5001/webman/login/dist/dsm.login.bundle.js (v [1661421011]
↪ )
https://93.11.145.199:5001/webman/login/dist/style.css (v [1661421011] )
https://93.11.145.199:5001/webman/modules/ActiveInsightUpdateNotify/style.css (v
```

... continues on next page ...

... continued from previous page ...

```
↪ [1661421011] )
https://93.11.145.199:5001/webman/modules/AdminCenter/style.css (v [1661226912]
↪)
https://93.11.145.199:5001/webman/modules/AudioPlayer/style.css (v [1661757678]
↪)
https://93.11.145.199:5001/webman/modules/BackgroundTaskMonitor/style.css (v [16
↪61757678] )
https://93.11.145.199:5001/webman/modules/BandwidthControl/style.css (v [1634102
↪886] )
https://93.11.145.199:5001/webman/modules/C3/style.css (v [1661421011] )
https://93.11.145.199:5001/webman/modules/ClipBoardJS/style.css (v [1661757678]
↪)
https://93.11.145.199:5001/webman/modules/ConfigBackup/style.css (v [1660704937]
↪ )
https://93.11.145.199:5001/webman/modules/DSMNotify/style.css (v [1661757678] )
https://93.11.145.199:5001/webman/modules/DataDrivenDocuments/style.css (v [1661
↪421011] )
https://93.11.145.199:5001/webman/modules/DesktopProgress/style.css (v [16617576
↪78] )
https://93.11.145.199:5001/webman/modules/DisableAdminNotification/style.css (v
↪[1661421011] )
https://93.11.145.199:5001/webman/modules/DiskMessageHandler/style.css (v [16614
↪21011] )
https://93.11.145.199:5001/webman/modules/EnableNewUpdateSetting/style.css (v [1
↪661421011] )
https://93.11.145.199:5001/webman/modules/ExternalDevices/style.css (v [16614210
↪11] )
https://93.11.145.199:5001/webman/modules/FileChooser/style.css (v [1661757678]
↪)
https://93.11.145.199:5001/webman/modules/FileChooserV6/style.css (v [1661757678
↪] )
https://93.11.145.199:5001/webman/modules/HelpBrowser/style.css (v [1661757678]
↪)
https://93.11.145.199:5001/webman/modules/HotkeyManager/style.css (v [1661421011
↪] )
https://93.11.145.199:5001/webman/modules/LogCenter/style.css (v [1657013615] )
https://93.11.145.199:5001/webman/modules/MyDSCenter/style.css (v [1661757678] )
https://93.11.145.199:5001/webman/modules/OTPWizard/style.css (v [1661757678] )
https://93.11.145.199:5001/webman/modules/PersonalSettings/style.css (v [1661757
↪678] )
https://93.11.145.199:5001/webman/modules/PhotoViewer/style.css (v [1661757678]
↪)
https://93.11.145.199:5001/webman/modules/PkgManApp/style.css (v [1661757678] )
https://93.11.145.199:5001/webman/modules/PollingTask/style.css (v [1661757678]
↪)
https://93.11.145.199:5001/webman/modules/ResetAdminApp/style.css (v [1661421011
↪] )
```

... continues on next page ...

... continued from previous page ...

https://93.11.145.199:5001/webman/modules/ResourceMonitor/style.css (v [16614210
↪11])
https://93.11.145.199:5001/webman/modules/SecurityScan/style.css (v [1652943644]
↪)
https://93.11.145.199:5001/webman/modules/Share/style.css (v [1661757678])
https://93.11.145.199:5001/webman/modules/SharingManager/style.css (v [166175767
↪8])
https://93.11.145.199:5001/webman/modules/StorageManager/style.css (v [166142101
↪1])
https://93.11.145.199:5001/webman/modules/SupportForm/style.css (v [1661757678]
↪)
https://93.11.145.199:5001/webman/modules/SystemInfoApp/style.css (v [1661421011
↪])
https://93.11.145.199:5001/webman/modules/TaskSchedulerUtils/style.css (v [16617
↪57678])
https://93.11.145.199:5001/webman/modules/TaskSchedulerWidget/style.css (v [1661
↪421011])
https://93.11.145.199:5001/webman/modules/TinyMCE/style.css (v [1635321605])
https://93.11.145.199:5001/webman/modules/UpdateMaskApp/style.css (v [1661421011
↪])
https://93.11.145.199:5001/webman/modules/Utils/style.css (v [1661757678])
https://93.11.145.199:5001/webman/modules/VideoPlayer2/style.css (v [1649656611]
↪)
https://93.11.145.199:5001/webman/modules/WelcomeApp/style.css (v [1661421011])
https://93.11.145.199:5001/webman/modules/Widgets/style.css (v [1661421011])
https://93.11.145.199:5001/webman/resources/css/desktop.css (v [1661421011])
https://93.11.145.199:5001/webman/sds/dist/dsm.common.bundle.js (v [1661421011]
↪)
https://93.11.145.199:5001/webman/sds/dist/dsm.sds.bundle.js (v [1661421011])
https://93.11.145.199:5001/webman/taskbar/dist/dsm.taskbar.bundle.js (v [1661421
↪011])
https://93.11.145.199:5001/webman/taskbar/dist/style.css (v [1661421011])
https://93.11.145.199:5001/webman/unsupported-browsers/dist/bundle.css (v [16614
↪21011])
https://93.11.145.199:5001/webman/unsupported-browsers/dist/bundle.js (v [166142
↪1011])

Solution:

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2023-03-03T10:59:40Z

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

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 | base-uri 'self';  connect-src data
X-Content-Type-Options  | nosniff
X-Frame-Options         | SAMEORIGIN
X-XSS-Protection        | 1; mode=block
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
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
```

... continues on next page ...

... continued from previous page ...

```
↪/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
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-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
```

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: HTTP Server Banner Enumeration

Summary
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).

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner | Enumeration technique
--------------------------------------------------------------------------------
Server: nginx | Invalid HTTP 00.5 GET request (non-existent HTTP version) 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: HTTP Server type and version

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

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: nginx`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2020-08-24T15:18:35Z`

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://93.11.145.199:5001/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: 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

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

... continues on next page ...

... continued from previous page ...

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:
fingerprint (SHA-1)             | 779927C6709692C50A863F94CE8786D611DE9947
fingerprint (SHA-256)           | C9C64376788DA928E598B22CFD290DC46F13D961035095
↪57CC730EA48A1110C9
issued by                       | CN=Synology Inc. CA,O=Synology Inc.,L=Taipei,C
↪=TW
public key size (bits)          | 2048
serial                          | 63EA9D1E860CA532C7A04BE011EDF3DB9CBA91D8
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=synology,O=Synology Inc.,L=Taipei,C=TW
subject alternative names (SAN) | synology
valid from                      | 2022-11-28 18:26:52 UTC
valid until                     | 2023-11-29 18:26:52 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: 2023-02-17T10:09:43Z

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
Server: nginx
Date: ***replaced***
Content-Type: text/html; charset="UTF-8"
Transfer-Encoding: chunked
```

... continues on next page ...

... continued from previous page ...

```
Connection: close
Cache-control: no-store
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Content-Security-Policy: base-uri 'self';  connect-src data: ws: wss: http: http
↪s:; default-src 'self' 'unsafe-eval' data: blob: https://*.synology.com https:
↪//www.synology.cn/ https://help.synology.cn/; font-src 'self' data: https://*.
↪googleapis.com https://*.gstatic.com; form-action 'self'; frame-ancestors 'sel
↪f'; frame-src 'self' data: blob: https://*.synology.com https://*.synology.cn;
↪ img-src 'self' data: blob: https://*.google.com https://*.googleapis.com http
↪://*.googlecode.com https://*.gstatic.com https://global.download.synology.com
↪; media-src 'self' data: about: https://*.synology.com https://help.synology.c
↪n;  script-src 'self' 'unsafe-eval' data: blob: https://maps.google.com https:
↪//ajax.googleapis.com https://help.synology.com https://help.synology.cn; styl
↪e-src 'self' 'unsafe-inline' https://*.googleapis.com;
```

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-
↪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: 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
Server: nginx
Date: ***replaced***
Content-Type: text/html; charset="UTF-8"
Transfer-Encoding: chunked
Connection: close
Cache-control: no-store
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Content-Security-Policy: base-uri 'self';  connect-src data: ws: wss: http: http
↪s:; default-src 'self' 'unsafe-eval' data: blob: https://*.synology.com https:
↪//www.synology.cn/ https://help.synology.cn/; font-src 'self' data: https://*.
↪googleapis.com https://*.gstatic.com; form-action 'self'; frame-ancestors 'sel
↪f'; frame-src 'self' data: blob: https://*.synology.com https://*.synology.cn;
↪ img-src 'self' data: blob: https://*.google.com https://*.googleapis.com http
↪://*.googlecode.com https://*.gstatic.com https://global.download.synology.com
↪; media-src 'self' data: about: https://*.synology.com https://help.synology.c
↪n;  script-src 'self' 'unsafe-eval' data: blob: https://maps.google.com https:
↪//ajax.googleapis.com https://help.synology.com https://help.synology.cn; styl
↪e-src 'self' 'unsafe-inline' https://*.googleapis.com;
```

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

... continues on next page ...

... continued from previous page ...

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_Transport_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
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: 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.

Vulnerability Detection Result

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

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: 2022-09-22T10:44:54Z

References

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

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_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_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: 2021-12-01T13:10:37Z

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_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_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: 2021-12-01T09:24:41Z

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 TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
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
TLS_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: 2021-12-09T13:40:52Z

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

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

Vulnerability Detection Result
```
'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_GCM_SHA256
TLS_ECDHE_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:
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
```

... continues on next page ...

... continued from previous page ...

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: 2022-08-25T10:12:37Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Untrusted Certificate Detection

Summary
Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.

Vulnerability Detection Result
The remote SSL/TLS server is using the following certificate(s) which failed the
↪ verification against the system wide trust store (serial:issuer):
63EA9D1E860CA532C7A04BE011EDF3DB9CBA91D8:CN=Synology Inc. CA,O=Synology Inc.,L=T
↪aipei,C=TW (Server certificate)

Solution:

Log Method
Details: SSL/TLS: Untrusted Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.117764
Version used: 2021-11-12T09:42:39Z

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

Summary

... continues on next page ...

... continued from previous page ...

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

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
Version used: `2021-12-06T15:42:24Z`

[return to 93.11.145.199]

2.1.4 Log 80/tcp

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 forum.

Vulnerability Detection Result

```
The Hostname/IP "93.11.145.199" 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.
```

... continues on next page ...

... continued from previous page ...

```
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)" 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://93.11.145.199/
http://93.11.145.199/.well-known/acme-challenge
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: 2023-03-03T10:59:40Z

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

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

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪--------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
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
```

... continues on next page ...

... continued from previous page ...

```
↪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
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-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-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: 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).

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner | Enumeration technique
--------------------------------------------------------------------------------
Server: nginx | Invalid HTTP 00.5 GET request (non-existent HTTP version) 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: HTTP Server type and version

Summary

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

Vulnerability Detection Result

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

Solution:

Log Method

Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2020-08-24T15:18:35Z`

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

... continues on next page ...

... continued from previous page ...

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 93.11.145.199]

2.1.5 Log 443/tcp

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 forum.

Vulnerability Detection Result
The Hostname/IP "93.11.145.199" 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 NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)" 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://93.11.145.199/

... continues on next page ...

... continued from previous page ...

https://93.11.145.199/.well-known/acme-challenge
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: 2023-03-03T10:59:40Z

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

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

Missing Headers	More Information
Content-Security-Policy	https://owasp.org/www-project-secure-headers/#content-security-policy
Cross-Origin-Embedder-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Opener-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Resource-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Document-Policy	https://w3c.github.io/webappsec-feature-policy/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 Permissions Policy
Permissions-Policy	https://w3c.github.io/webappsec-feature-policy/#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
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-Frame-Options                  | https://owasp.org/www-project-secure-headers
↪/#x-frame-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: HTTP Server Banner Enumeration

... continues on next page ...

... continued from previous page ...

Summary
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).

Vulnerability Detection Result
```
It was possible to enumerate the following HTTP server banner(s):
Server banner | Enumeration technique
--------------------------------------------------------------------------------
Server: nginx | Invalid HTTP 00.5 GET request (non-existent HTTP version) 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: HTTP Server type and version

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

Vulnerability Detection Result
```
The remote HTTP Server banner is:
Server: nginx
```

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2020-08-24T15:18:35Z`

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.

... continues on next page ...

... continued from previous page ...

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

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:
fingerprint (SHA-1)             | 779927C6709692C50A863F94CE8786D611DE9947
fingerprint (SHA-256)           | C9C64376788DA928E598B22CFD290DC46F13D961035095
↪57CC730EA48A1110C9
issued by                       | CN=Synology Inc. CA,O=Synology Inc.,L=Taipei,C
↪=TW
```

... continues on next page ...

... continued from previous page ...

public key size (bits)	2048
serial	63EA9D1E860CA532C7A04BE011EDF3DB9CBA91D8
signature algorithm	sha256WithRSAEncryption
subject	CN=synology,O=Synology Inc.,L=Taipei,C=TW
subject alternative names (SAN)	synology
valid from	2022-11-28 18:26:52 UTC
valid until	2023-11-29 18:26:52 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: 2023-02-17T10:09:43Z

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/1.1 403 Forbidden
Server: nginx
Date: ***replaced***
Content-Type: text/html
Content-Length: ***replaced***
Connection: close
ETag: "***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.

... continues on next page ...

... continued from previous page ...

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-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: 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/1.1 403 Forbidden
Server: nginx
Date: ***replaced***
Content-Type: text/html
Content-Length: ***replaced***
Connection: close
ETag: "***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

... continues on next page ...

... continued from previous page ...

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_Transport_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
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: 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.

Vulnerability Detection Result
The remote service advertises support for the following Network Protocol(s) via the NPN extension:
SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1
TLSv1.2:HTTP/2
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
TLSv1.2:HTTP/2

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: 2022-09-22T10:44:54Z

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

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_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_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: 2021-12-01T13:10:37Z

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_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_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: 2021-12-01T09:24:41Z

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 TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
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
TLS_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: 2021-12-09T13:40:52Z

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

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

Vulnerability Detection Result
```
'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_GCM_SHA256
TLS_ECDHE_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:
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
```

... continues on next page ...

... continued from previous page ...

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: 2022-08-25T10:12:37Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Untrusted Certificate Detection

Summary
Checks and reports if a remote SSL/TLS service is using a certificate which is untrusted / the verification against the system wide trust store has failed.

Vulnerability Detection Result
The remote SSL/TLS server is using the following certificate(s) which failed the
↪ verification against the system wide trust store (serial:issuer):
63EA9D1E860CA532C7A04BE011EDF3DB9CBA91D8:CN=Synology Inc. CA,O=Synology Inc.,L=T
↪aipei,C=TW (Server certificate)

Solution:

Log Method
Details: SSL/TLS: Untrusted Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.117764
Version used: 2021-11-12T09:42:39Z

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

Summary

... continues on next page ...

... continued from previous page ...

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

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
Version used: `2021-12-06T15:42:24Z`

[return to 93.11.145.199]

2.1.6 Log general/tcp

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 93.11.145.199:`
`Hostname|Source`
`93.11.145.199|IP-address`

Solution:

Log Method
Details: `Hostname Determination Reporting`
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: `2022-07-27T10:11:28Z`

Log (CVSS: 0.0)
NVT: nginx Detection Consolidation

... continues on next page ...

... continued from previous page ...

Summary
Consolidation of nginx detections.

Vulnerability Detection Result

```
Detected nginx
Version:       unknown
Location:      443/tcp
CPE:           cpe:/a:nginx:nginx
Concluded from version/product identification result:
Server: nginx
Detected nginx
Version:       unknown
Location:      5000/tcp
CPE:           cpe:/a:nginx:nginx
Concluded from version/product identification result:
Server: nginx
Detected nginx
Version:       unknown
Location:      5001/tcp
CPE:           cpe:/a:nginx:nginx
Concluded from version/product identification result:
Server: nginx
Detected nginx
Version:       unknown
Location:      80/tcp
CPE:           cpe:/a:nginx:nginx
Concluded from version/product identification result:
Server: nginx
```

Solution:

Log Method
Details: `nginx Detection Consolidation`
OID:1.3.6.1.4.1.25623.1.0.113787
Version used: `2022-02-03T09:26:44Z`

References
`url: https://www.nginx.com/`

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.

... continues on next page ...

... continued from previous page ...

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.

Vulnerability Detection Result

```
Best matching OS:
OS:           Synology DiskStation Manager
CPE:          cpe:/o:synology:unknown_model_firmware:7.1.1-42962
Found by NVT: 1.3.6.1.4.1.25623.1.0.170202 (Synology NAS / DiskStation Manager (
↪DSM) Detection Consolidation)
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: `2023-03-03T10:59:40Z`

References

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

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 but not resolvable hostnames were detected:
synology
```

Solution:

Log Method

Details: `SSL/TLS: Hostname discovery from server certificate`
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: `2021-11-22T15:32:39Z`

... continues on next page ...

... continued from previous page ...

Log (CVSS: 0.0)
NVT: Synology NAS / DiskStation Manager (DSM) Detection Consolidation

Summary
Consolidation of Synology NAS devices, DiskStation Manager (DSM) OS and application detections.

Vulnerability Detection Result

```
Detected Synology NAS Unknown Model Firmware
Version:       7.1.1-42962
Location:      /
CPE:           cpe:/o:synology:unknown_model_firmware:7.1.1-42962
Detected Synology NAS Unknown Model Device
Location:      /
CPE:           cpe:/h:synology:unknown_model
Detected Synology DiskStation Manager
Location:      /
CPE:           cpe:/a:synology:diskstation_manager:7.1.1-42962
Detection methods:
HTTP(s) on port 5001/tcp
  Concluded:
    productversion="7.1.1"
    buildnumber="42962"
  from URL(s):
    https://93.11.145.199:5001/index.cgi
    https://93.11.145.199:5001/synohdpack/synohdpack.version
```

Solution:

Log Method
Details: Synology NAS / DiskStation Manager (DSM) Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.170202
Version used: 2022-12-21T10:12:09Z

References
url: https://www.synology.com/en-us/dsm

Log (CVSS: 0.0)
NVT: Traceroute

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Network route from scanner (10.88.0.7) to target (93.11.145.199):
10.88.0.7
10.206.6.181
10.206.35.31
10.206.32.2
173.255.239.102
198.32.160.112
195.2.25.70
195.2.24.242
195.2.9.133
195.89.97.142
194.6.143.235
86.69.254.5
93.11.145.199
Network distance between scanner and target: 13
```

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`

[return to 93.11.145.199]

2.1.7 Log 5000/tcp

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

... continues on next page ...

... continued from previous page ...

- 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.

Vulnerability Detection Result

```
The Hostname/IP "93.11.145.199" 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 NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)" 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://93.11.145.199:5000/
http://93.11.145.199:5000/oauth
http://93.11.145.199:5000/scripts
http://93.11.145.199:5000/synoSDSjslib
http://93.11.145.199:5000/synohdpack
http://93.11.145.199:5000/webapi
http://93.11.145.199:5000/webman
http://93.11.145.199:5000/webman/3rdparty
http://93.11.145.199:5000/webman/modules
http://93.11.145.199:5000/webman/resources
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: 2023-03-03T10:59:40Z

References

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

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

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
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
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
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-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
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: 2021-07-14T06:19:43Z

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: HTTP Server Banner Enumeration

Summary
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).

Vulnerability Detection Result
It was possible to enumerate the following HTTP server banner(s):
Server banner | Enumeration technique

Server: nginx | Invalid HTTP 00.5 GET request (non-existent HTTP version) 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: HTTP Server type and version

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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: nginx

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2020-08-24T15:18:35Z

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://93.11.145.199:5000/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

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

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 93.11.145.199]