Scan Report

June 7, 2021

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “windows_highest_Port setting”. The scan started at Mon Jun 7 07:55:31 2021 UTC and ended at Mon Jun 7 08:07:04 2021 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.178.49 sn-desktop.fritz.box	0	0	0	12	0
Total: 1	0	0	0	12	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “High” are not shown.
Issues with the threat level “Medium” are not shown.
Issues with the threat level “Low” are not shown.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 12 results selected by the filtering described above. Before filtering there were 13 results.

2 Results per Host

2.1 192.168.178.49

Host scan start	Mon Jun 7 07:55:54 2021 UTC
Host scan end	Mon Jun 7 08:06:59 2021 UTC

Service (Port)	Threat Level
general/tcp	Log
general/CPE-T	Log
60286/tcp	Log
65245/tcp	Log
62634/tcp	Log
80/tcp	Log

2.1.1 Log general/tcp

Log (CVSS: 0.0)
NVT: Traceroute

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

Vulnerability Detection Result

```
Network route from scanner (10.0.2.15) to target (192.168.178.49):
10.0.2.15
192.168.178.49
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: `2021-03-12T14:25:59Z`

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

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

Vulnerability Detection Result

```
Best matching OS:
OS:           HP JetDirect
CPE:          cpe:/h:hp:jetdirect
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICM
↪P))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:

Log Method

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

References

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

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary

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

Vulnerability Detection Result

```
Hostname determination for IP 192.168.178.49:
Hostname|Source
sn-desktop.fritz.box|Reverse-DNS
```

Solution:

Log Method

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

[return to 192.168.178.49]

2.1.2 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.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
192.168.178.49|cpe:/a:microsoft:internet_information_services:10.0
192.168.178.49|cpe:/h:hp:jetdirect
```

Solution:

Log Method

Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2021-04-16T10:39:13Z`

References

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

[return to 192.168.178.49]

2.1.3 Log 60286/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary

This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Solution:

Log Method

Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `2019-02-20T11:12:24Z`

[return to 192.168.178.49]

2.1.4 Log 65245/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Solution:

Log Method
Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `2019-02-20T11:12:24Z`

[return to 192.168.178.49]

2.1.5 Log 62634/tcp

Log (CVSS: 0.0)
NVT: Check open ports

Summary
This plugin checks if the port scanners did not kill a service.

Vulnerability Detection Result

```
This port was detected as being open by a port scanner but is now closed.
This service might have been crashed by a port scanner or by a plugin
```

Solution:

Log Method
Details: `Check open ports`
OID:1.3.6.1.4.1.25623.1.0.10919
Version used: `2019-02-20T11:12:24Z`

[return to 192.168.178.49]

2.1.6 Log 80/tcp

Log (CVSS: 0.0)
NVT: Microsoft Internet Information Services (IIS) Detection (HTTP)

Summary
HTTP based detection of Microsoft Internet Information Services (IIS).

Vulnerability Detection Result

```
Detected Microsoft Internet Information Services (IIS)
Version:       10.0
Location:      80/tcp
CPE:           cpe:/a:microsoft:internet_information_services:10.0
Concluded from version/product identification result:
Server: Microsoft-IIS/10.0
```

Solution:

Log Method
Details: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.900710
Version used: `2021-03-11T14:24:14Z`

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: Microsoft-IIS/10.0
```

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: 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: Microsoft-HTTPAPI/2.0 | Valid HTTP 0.9 GET request to '/index.html'
Server: Microsoft-IIS/10.0    | Valid HTTP 1.0 GET request to '/index.htm'
```

Solution:

Log Method

Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2021-01-11T11:29:35Z`

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary

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

If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "sn-desktop.fritz.box" 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.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
The following directories were used for CGI scanning:
http://sn-desktop.fritz.box/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

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

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

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

Summary
All known security headers are being checked on the remote web server.
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
Document-Policy                  | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                   | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy               | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                  | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
X-Content-Type-Options           | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-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 suppor
↪t for this header in 2020.
```

Solution:

Log Method

Details: `HTTP Security Headers Detection`

OID:1.3.6.1.4.1.25623.1.0.112081

Version used: `2021-01-26T13:20:44Z`

References

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

[return to 192.168.178.49]

This file was automatically generated.