Scan Report

August 20, 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 "StudentWellness". The scan started at Sun Aug 20 17:40:11 2023 UTC and ended at Sun Aug 20 17:49:20 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
192.168.50.172 studentwellness	0	0	0	4	0
Total: 1	0	0	0	4	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 4 results selected by the filtering described above. Before filtering there were 4 results.

2 Results per Host

2.1 192.168.50.172

Host scan start	Sun Aug 20 17:40:12 2023 UTC
Host scan end	Sun Aug 20 17:49:17 2023 UTC

Service (Port)	Threat Level
22/tcp	Log
443/tcp	Log
general/tcp	Log
80/tcp	Log

2.1.1 Log 22/tcp

Log (CVSS: 0.0)
NVT: Services

Summary

. . . continues on next page . . .

... continued from previous page ...

This plugin performs service detection.

Vulnerability Detection Result
`An ssh server is running on this port`

Solution:

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

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

[return to 192.168.50.172]

2.1.2 Log 443/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

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

Solution:

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

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

[return to 192.168.50.172]

2.1.3 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 192.168.50.172:`
`Hostname|Source`
`studentwellness|Reverse-DNS`

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`

[return to 192.168.50.172]

2.1.4 Log 80/tcp

Log (CVSS: 0.0) NVT: Services
Summary This plugin performs service detection.
Vulnerability Detection Result `A web server is running on this port`
Solution:
Vulnerability Insight This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Log Method Details: `Services` OID:1.3.6.1.4.1.25623.1.0.10330
. . . continues on next page . . .

... continued from previous page ...

Version used: 2023-06-14T05:05:19Z

[return to 192.168.50.172]
