Scan Report

May 26, 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 "ubuntu11". The scan started at Wed May 26 08:03:47 2021 UTC and ended at Wed May 26 08:05:38 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
10.10.10.2	0	0	0	6	0
Total: 1	0	0	0	6	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 6 results selected by the filtering described above. Before filtering there were 6 results.

2   Results per Host

2.1   10.10.10.2

Host scan start   Wed May 26 08:04:12 2021 UTC
Host scan end   Wed May 26 08:05:36 2021 UTC

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

2.1.1   Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary

. . . continues on next page . . .

... continued from previous page ...

The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution:

Log Method
Details: `ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2021-03-23T06:51:29Z`

References
cve: `CVE-1999-0524`
url: `http://www.ietf.org/rfc/rfc0792.txt`
cert-bund: `CB-K15/1514`
cert-bund: `CB-K14/0632`
dfn-cert: `DFN-CERT-2014-0658`

2.1.2   Log general/tcp

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

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

Vulnerability Detection Result
```
Best matching OS:
OS:           Linux Kernel
CPE:          cpe:/o:linux:kernel
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
```
... continues on next page ...

Setting key "Host/runs_unixoide" based on this information

Solution:

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

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

Log (CVSS: 0.0)
NVT: Check for enabled / working Port scanner plugin

Summary The script reports if: - a custom scan configuration is in use without having a Port scanner from the 'Port scanners' family enabled. - a port scanner plugin was running into a timeout. - a required port scanner (e.g. nmap) is not installed.

Vulnerability Detection Result The host wasn't scanned due to the following possible reasons: - No Port scanner plugin from the "Port scanners" family is included in this sc ↪an configuration. Recommended: Nmap (NASL wrapper). - The Port scanner plugin reached a timeout during the port scanning phase. Ple ↪ase either choose a port range for this target containing less ports or raise ↪the "scanner_plugins_timeout" scanner preference to a higher timeout.

Solution: Based on the script output please: - add a Port scanner plugin from the 'Port scanners' family to this scan configuration. Recommended: Nmap (NASL wrapper). - either choose a port range for this target containing less ports or raise the 'scanner_plugins_timeout' scanner preference to a higher timeout. - install the 'nmap' binary/package or make it accessible to the scanner.

Log Method Details: Check for enabled / working Port scanner plugin OID:1.3.6.1.4.1.25623.1.0.108323 Version used: 2021-03-23T06:51:29Z

References

```
url: https://docs.greenbone.net/GSM-Manual/gos-20.08/en/performance.html#optimiz
↪ing-the-scan-performance
url: https://docs.greenbone.net/GSM-Manual/gos-20.08/en/scanning.html?highlight=
↪scanner_plugins_timeout#description-of-scanner-preferences
```

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 (10.10.10.3) to target (10.10.10.2):
10.10.10.3
10.10.10.2
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: Hostname Determination Reporting

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

Vulnerability Detection Result
```
Hostname determination for IP 10.10.10.2:
Hostname|Source
10.10.10.2|IP-address
```

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`

2.1.3   Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

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

Vulnerability Detection Result
`10.10.10.2|cpe:/o:linux:kernel`

Solution:

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

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

This file was automatically generated.