Scan Report

August 6, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "metaspoitable scan". The scan started at Tue Aug 6 16:56:11 2024 UTC and ended at Tue Aug 6 17:22:55 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.10 kali.domain.name	0	1	1	0	0
Total: 1	0	1	1	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.
It only lists hosts that produced issues.
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 2 results selected by the filtering described above. Before filtering there were 18 results.

Results per Host

192.168.1.10

Host scan start	Tue Aug 6 16:57:06 2024 UTC
Host scan end	Tue Aug 6 17:22:52 2024 UTC

Service (Port)	Threat Level
443/tcp	Medium
general/tcp	Low

Medium 443/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result
`The certificate of the remote service expired on 2020-08-20 19:18:24.`
`Certificate details:`

... continues on next page ...

... continued from previous page ...

```
subject ...: C=DE,L=Osnabrueck,O=OpenVAS Users,CN=218ffb30ff7a
subject alternative names (SAN):
None
issued by .: C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for 218f
↪fb30ff7a
serial ....: 5B7C65801F8422EBBDAD2299
valid from : 2018-08-21 19:18:24 UTC
valid until: 2020-08-20 19:18:24 UTC
fingerprint (SHA-1): 6B34D170BC2D0EAE4DB2D6122E2DA7E94F0ADF6F
fingerprint (SHA-256): A672ACF69BB0944271599E210BF04BF20736E3CCB5862FAF3EFAC9872
↪41BC4B9
```

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `$Revision: 11103 $`

[return to 192.168.1.10]

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.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 728572811
Packet 2: 728575192
```

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

Solution
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

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/IPv4 implementations that implement RFC1323.

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

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: `$Revision: 14310 $`

References
`Other:`
`URL:http://www.ietf.org/rfc/rfc1323.txt`
`URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152`

[return to 192.168.1.10]