Scan Report

March 23, 2020

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 "admin.tanca.io". The scan started at Mon Mar 23 13:28:49 2020 UTC and ended at Mon Mar 23 13:41:28 2020 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
103.48.191.148 admin.tanca.io	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 40 results.

Host Authentications

Host	Protocol	Result	Port/User
103.48.191.148 - admin.tanca.io	SSH	Failure	Protocol SSH, Port 62636, User root : Login failure

Results per Host

103.48.191.148

Host scan start	Mon Mar 23 13:29:21 2020 UTC
Host scan end	Mon Mar 23 13:41:28 2020 UTC

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

Medium 443/tcp

Medium (CVSS: 5.0) NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
. . . continues on next page . . .

... continued from previous page ...

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: $Revision: 5232 $

References
CVE: CVE-2016-2183, CVE-2016-6329
Other:
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
URL:https://sweet32.info/

[return to 103.48.191.148]

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: 1164385611
Packet 2: 1164386739
```

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/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 103.48.191.148]