Scan Report

November 30, 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 "STEPES-TR". The scan started at Mon Nov 30 00:18:01 2020 UTC and ended at Mon Nov 30 01:52:57 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

1 Result Overview

Host	High	Medium	Low	Log	False Positive
54.196.179.100 ec2-54-196-179-100.compute-1.amazonaws.com	0	1	1	0	0
Total: 1	0	1	1	0	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 “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 75 results.

2 Results per Host

2.1 54.196.179.100

Host scan start	Mon Nov 30 00:18:04 2020 UTC
Host scan end	Mon Nov 30 01:51:54 2020 UTC

Service (Port)	Threat Level
1883/tcp	Medium
general/tcp	Low

2.1.1 Medium 1883/tcp

Medium (CVSS: 6.4)
NVT: MQTT Broker Does Not Require Authentication

Summary
The remote MQTT does not require authentication.

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

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: Mitigation

Enable authentication.

Vulnerability Detection Method

Connect to the remote MQTT broker and check if authentication is needed.

Details: `MQTT Broker Does Not Require Authentication`

OID:1.3.6.1.4.1.25623.1.0.140167

References

```
url: https://www.heise.de/newsticker/meldung/MQTT-Protokoll-IoT-Kommunikation-vo
↪n-Reaktoren-und-Gefaengnissen-oeffentlich-einsehbar-3629650.html
```

[return to 54.196.179.100]

2.1.2 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/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 2932734514
Packet 2: 2932735766
```

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 implementations that implement RFC1323/RFC7323.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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

References

```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 54.196.179.100]

This file was automatically generated.