Scan Report

July 11, 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 “Prueba Local”. The scan started at Tue Jul 11 15:18:24 2023 UTC and ended at Tue Jul 11 15:25:22 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 2
2 Results per Host 2
  2.1 127.0.0.1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
    2.1.1 High general/tcp . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
    2.1.2 Medium 1883/tcp . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
1 Result Overview

<table>
<thead>
<tr>
<th>Host</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Log</th>
<th>False Positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total: 1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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 13 results.

2 Results per Host

2.1 127.0.0.1

Host scan start Tue Jul 11 15:18:52 2023 UTC
Host scan end Tue Jul 11 15:25:17 2023 UTC

<table>
<thead>
<tr>
<th>Service (Port)</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>general/tcp</td>
<td>High</td>
</tr>
<tr>
<td>1883/tcp</td>
<td>Medium</td>
</tr>
</tbody>
</table>

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Report outdated / end-of-life Scan Engine / Environment (local)

Summary
This script checks and reports an outdated or end-of-life scan engine for the following environments:
- Greenbone Community Edition
- Greenbone Enterprise TRIAL (formerly Greenbone Security Manager TRIAL / Greenbone Community Edition VM)

...continues on next page...
NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make
you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the
target due to e.g.:
- missing functionalities
- missing bugfixes
- incompatibilities within the feed

Vulnerability Detection Result

Version of installed component: 22.4.1 (Installed component: openvas libraries on OpenVAS <= 9, openvas-scanner on Greenbone Community Edition >= 10)

Latest available openvas-scanner version: 22.7.2

Solution:

Solution type: VendorFix
Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.

If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked GSM manual.

Vulnerability Detection Method

Details: Report outdated / end-of-life Scan Engine / Environment (local)
OID: 1.3.6.1.4.1.25623.1.0.108560

Version used: 2023-07-04T05:05:35Z

References

url: https://www.greenbone.net/en/testnow/
url: https://forum.greenbone.net/t/gvm-20-08-end-of-life-initial-release-2020-08-12/6312
url: https://forum.greenbone.net/t/gvm-11-end-of-life-initial-release-2019-10-14/3674
2.1.2 Medium 1883/tcp

<table>
<thead>
<tr>
<th>Medium (CVSS: 6.4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVT: MQTT Broker Does Not Require Authentication</td>
</tr>
</tbody>
</table>

**Summary**
The remote MQTT broker does not require authentication.

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

**Solution:**
Solution type: Mitigation
Enable authentication.

**Vulnerability Detection Method**
Checks if authentication is required for the remote MQTT broker.
Details: MQTT Broker Does Not Require Authentication
OID:1.3.6.1.4.1.25623.1.0.140167
Version used: 2022-07-11T10:16:03Z

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

This file was automatically generated.