Scan Report

March 2, 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 “Immediate scan of IP 127.0.0.1”. The scan started at Thu Mar 2 23:18:21 2023 UTC and ended at Thu Mar 2 23:21:07 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

Host	High	Medium	Low	Log	False Positive
127.0.0.1 localhost	1	0	0	0	0
Total: 1	1	0	0	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 result 1 of the 1 results selected by the filtering above. Before filtering there were 19 results.

2 Results per Host

2.1 127.0.0.1

Host scan start	Thu Mar 2 23:18:46 2023 UTC
Host scan end	Thu Mar 2 23:21:07 2023 UTC

Service (Port)	Threat Level
9390/tcp	High

2.1.1 High 9390/tcp

High (CVSS: 10.0)
NVT: OpenVAS / Greenbone Vulnerability Manager Default Credentials

Product detection result

```
cpe:/a:openvas:openvas_manager:7.0
Detected by OpenVAS / Greenbone Vulnerability Manager Detection (OID: 1.3.6.1.4.
↪1.25623.1.0.103825)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.

Vulnerability Detection Result

```
It was possible to login using the following credentials (username:password:role
↪):
admin:admin:Admin
```

Impact

This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution

Solution type: Workaround

Change the password of the mentioned account(s).

Vulnerability Insight

It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.

Vulnerability Detection Method

Try to login with default credentials via the OMP/GMP protocol.

Details: `OpenVAS / Greenbone Vulnerability Manager Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.108554

Version used: `$Revision: 13944 $`

Product Detection Result

Product: `cpe:/a:openvas:openvas_manager:7.0`

Method: `OpenVAS / Greenbone Vulnerability Manager Detection`

OID: 1.3.6.1.4.1.25623.1.0.103825)

[return to 127.0.0.1]

This file was automatically generated.