Scan Report

November 27, 2025

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 "grav3". The scan started at Thu Nov 27 00:17:12 2025 UTC and ended at Thu Nov 27 00:18:47 2025 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
127.0.0.1 localhost	0	0	0	2	0
Total: 1	0	0	0	2	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 "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 2 results.

Results per Host

127.0.0.1

Host scan start	Thu Nov 27 00:17:18 2025 UTC
Host scan end	Thu Nov 27 00:18:47 2025 UTC

Service (Port)	Threat Level
general/tcp	Log
general/CPE-T	Log

Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
Best matching OS:
OS: Linux Kernel
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Log Method

Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `$Revision: 14244 $`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

[return to 127.0.0.1]

Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary

This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

Vulnerability Detection Result

`127.0.0.1|cpe:/o:linux:kernel`

Log Method

Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 14324 $`

References

```
Other:
  URL:http://cpe.mitre.org/
```

[return to 127.0.0.1]