Scan Report

November 18, 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 “Localhost Vulnerability Scan”. The scan started at Tue Nov 18 10:55:29 2025 UTC and ended at Tue Nov 18 10:57:40 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

1 Result Overview **2**

2 Results per Host **2**

2.1 127.0.0.1 2

2.1.1 Medium 80/tcp 2

1 Result Overview

Host	High	Medium	Low	Log	False Positive
127.0.0.1	0	1	0	0	0
Total: 1	0	1	0	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 result 1 of the 1 results selected by the filtering above. Before filtering there were 24 results.

2 Results per Host

2.1 127.0.0.1

Host scan start	Tue Nov 18 10:55:36 2025 UTC
Host scan end	Tue Nov 18 10:57:36 2025 UTC

Service (Port)	Threat Level
80/tcp	Medium

2.1.1 Medium 80/tcp

Medium (CVSS: 5.3)

NVT: Apache HTTP Server /server-status Accessible (HTTP)

Summary
Requesting the URI /server-status provides information on the server activity and performance.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Vulnerable URL: http://localhost/server-status
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Requesting the URI /server-status gives throughout information about the currently running Apache to an attacker.

Solution:
Solution type: Mitigation
- If this feature is unused commenting out the appropriate section in the web servers configuration is recommended
- If this feature is used restricting access to trusted clients is recommended
- If the FreedomBox software is running on the target update the software to a later version

Affected Software/OS
- All Apache installations with an enabled 'mod_status' module
- FreedomBox through 20.13

Vulnerability Insight
server-status is a Apache HTTP Server handler provided by the 'mod_status' module and used to retrieve the server's activity and performance.

Vulnerability Detection Method
Checks if the /server-status page of Apache is accessible.
Details: `Apache HTTP Server /server-status Accessible (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.10677
Version used: `2023-10-13T05:06:10Z`

References
`cve: CVE-2020-25073`
`url: https://httpd.apache.org/docs/current/mod/mod_status.html`

[return to 127.0.0.1]