Scan Report

November 26, 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 "scan in grav 2". The scan started at Wed Nov 26 18:03:06 2025 UTC and ended at Wed Nov 26 18:20:51 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	2	0	0	0
Total: 1	0	2	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 all 2 results selected by the filtering described above. Before filtering there were 23 results.

Results per Host

127.0.0.1

Host scan start	Wed Nov 26 18:03:11 2025 UTC
Host scan end	Wed Nov 26 18:20:51 2025 UTC

Service (Port)	Threat Level
25/tcp	Medium
443/tcp	Medium

Medium 25/tcp

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

Vulnerability Detection Result
`'VRFY root' produces the following answer: 252 2.0.0 root`

... continues on next page ...

... continued from previous page ...

Solution
Solution type: Workaround
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: `Check if Mailserver answer to VRFY and EXPN requests`
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: `$Revision: 13470 $`

References
`Other:`
`URL:http://cr.yp.to/smtp/vrfy.html`

[return to 127.0.0.1]

Medium 443/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result
```
The certificate of the remote service expired on 2020-08-20 19:18:24.
Certificate details:
subject ...: C=DE,L=Osnabrueck,O=OpenVAS Users,CN=218ffb30ff7a
subject alternative names (SAN):
None
issued by .: C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for 218f
↪fb30ff7a
serial ....: 5B7C65801F8422EBBDAD2299
valid from : 2018-08-21 19:18:24 UTC
valid until: 2020-08-20 19:18:24 UTC
fingerprint (SHA-1): 6B34D170BC2D0EAE4DB2D6122E2DA7E94F0ADF6F
fingerprint (SHA-256): A672ACF69BB0944271599E210BF04BF20736E3CCB5862FAF3EFAC9872
↪41BC4B9
```

... continues on next page ...

... continued from previous page ...

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `$Revision: 11103 $`

[return to 127.0.0.1]