

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 “Immediate scan of IP 172.17.0.1”. The scan started at Thu Nov 27 01:26:53 2025 UTC and ended at Thu Nov 27 01:49:38 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	172.17.0.1	2
2.1.1	High 9390/tcp	2
2.1.2	Medium 443/tcp	3
2.1.3	Medium 9390/tcp	4
2.1.4	Medium 1111/tcp	5
2.1.5	Low general/tcp	7

Result Overview

Host	High	Medium	Low	Log	False Positive
172.17.0.1	1	4	1	0	0
Total: 1	1	4	1	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 6 results selected by the filtering described above. Before filtering there were 62 results.

Results per Host

172.17.0.1

Host scan start Thu Nov 27 01:26:58 2025 UTC
 Host scan end Thu Nov 27 01:49:38 2025 UTC

Service (Port)	Threat Level
9390/tcp	High
443/tcp	Medium
9390/tcp	Medium
1111/tcp	Medium
general/tcp	Low

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)
--

... continues on next page ...

... continued from previous page ...

Summary

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 172.17.0.1](#)]

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.

... continues on next page ...

	... continued from previous page ...
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	
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 172.17.0.1](#)]

Medium 9390/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
... continues on next page ...

<p style="text-align: right;">... continued from previous page ...</p> <pre>valid until: 2020-08-20 19:18:24 UTC fingerprint (SHA-1): 6B34D170BC2D0EAE4DB2D6122E2DA7E94F0ADF6F fingerprint (SHA-256): A672ACF69BB0944271599E210BF04BF20736E3CCB5862FAF3EFAC9872 →41BC4B9</pre>
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 172.17.0.1](#)]

Medium 1111/tcp

Medium (CVSS: 5.0) NVT: Missing 'httpOnly' Cookie Attribute
Summary The application is missing the 'httpOnly' cookie attribute
Vulnerability Detection Result The cookies: Set-Cookie: PHPSESSID=***replaced***; path=/ Set-Cookie: PHPSESSID=***replaced***; path=/ Set-Cookie: security=low are missing the "httpOnly" attribute.
Solution Solution type: Mitigation Set the 'httpOnly' attribute for any session cookie.
Affected Software/OS Application with session handling in cookies.
Vulnerability Insight The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method

Check all cookies sent by the application for a missing 'httpOnly' attribute

Details: Missing 'httpOnly' Cookie Attribute

OID:1.3.6.1.4.1.25623.1.0.105925

Version used: \$Revision: 5270 \$

References

Other:

URL:<https://www.owasp.org/index.php/HttpOnly>

URL:[https://www.owasp.org/index.php/Testing_for_cookies_attributes_\(OTG-SESS-002\)](https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002))

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

The following input fields where identified (URL:input name):

<http://172.17.0.1:1111/login.php>:password

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution

Solution type: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)

- HTTP Forms (e.g. Login) with input field of type 'password'

Details: Cleartext Transmission of Sensitive Information via HTTP

OID:1.3.6.1.4.1.25623.1.0.108440

... continues on next page ...

... continued from previous page ...
Version used: \$Revision: 10726 \$
References
Other:
URL: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management
URL: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
URL: https://cwe.mitre.org/data/definitions/319.html

[[return to 172.17.0.1](#)]

Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
Vulnerability Detection Result It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 127369047 Packet 2: 127370092
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution Solution type: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'. Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Affected Software/OS TCP/IPv4 implementations that implement RFC1323.
Vulnerability Insight The remote host implements TCP timestamps, as defined by RFC1323.
Vulnerability Detection Method ... continues on next page ...

... continued from previous page ...

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: TCP timestamps

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: \$Revision: 14310 \$

References

Other:

URL:<http://www.ietf.org/rfc/rfc1323.txt>

URL:<http://www.microsoft.com/en-us/download/details.aspx?id=9152>

[[return to 172.17.0.1](#)]

This file was automatically generated.