

# Scan Report

May 29, 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 “System Full Scan”. The scan started at Thu May 29 16:38:35 2025 UTC and ended at Thu May 29 16:45:08 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

<b>1</b>	<b>Result Overview</b>	<b>2</b>
<b>2</b>	<b>Results per Host</b>	<b>2</b>
2.1	127.0.0.1 . . . . .	2
2.1.1	Medium 5432/tcp . . . . .	2

## 1 Result Overview

Host	High	Medium	Low	Log	False Positive
127.0.0.1 localhost	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 27 results.

## 2 Results per Host

### 2.1 127.0.0.1

Host scan start Thu May 29 16:39:31 2025 UTC

Host scan end Thu May 29 16:45:05 2025 UTC

Service (Port)	Threat Level
5432/tcp	Medium

#### 2.1.1 Medium 5432/tcp

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

##### Product detection result

cpe:/a:ietf:transport\_layer\_security

Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.↔802067)

... continues on next page ...

...continued from previous page ...
<b>Summary</b> This routine reports all weak SSL/TLS cipher suites accepted by a service.
<b>Quality of Detection (QoD): 98%</b>
<b>Vulnerability Detection Result</b> 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_SEED_CBC_SHA
<b>Impact</b> This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.
<b>Solution:</b> <b>Solution type:</b> Mitigation The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.
<b>Affected Software/OS</b> All services providing an encrypted communication using weak SSL/TLS cipher suites.
<b>Vulnerability Insight</b> These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong
<b>Vulnerability Detection Method</b> Checks previous collected cipher suites. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication. Details: SSL/TLS: Report Weak Cipher Suites OID:1.3.6.1.4.1.25623.1.0.103440 Version used: 2025-03-27T05:38:50Z
<b>Product Detection Result</b> Product: cpe:/a:ietf:transport_layer_security Method: SSL/TLS: Report Supported Cipher Suites OID: 1.3.6.1.4.1.25623.1.0.802067)
... continues on next page ...

...continued from previous page ...

**References**

cve: CVE-2013-2566

cve: CVE-2015-2808

cve: CVE-2015-4000

url: <https://ssl-config.mozilla.org>

url: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html>

url: [https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/0TLS-Protokoll/TLS-Protokoll\\_node.html](https://www.bsi.bund.de/EN/Themen/0effentliche-Verwaltung/Mindeststandards/0TLS-Protokoll/TLS-Protokoll_node.html)

url: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>

url: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard\\_BSI\\_TLS\\_Version\\_2\\_4.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_4.html)

url: <https://web.archive.org/web/20240113175943/https://www.bettercrypto.org>

url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>

[\[ return to 127.0.0.1 \]](#)

---

This file was automatically generated.