# Nessus Essentials Vulnerability Scan Report for 127.0.0.1 (Localhost)

Date: June 26, 2025

Time: 12:00 PM IST

Tool Used: Nessus Essentials (Version 10.8)

Prepared by: shaunak kulkarni

Scan Performed: 12:00 PM IST, June 26, 2025

# 1 Summary

This report details the results of a vulnerability scan conducted on 127.0.0.1 (localhost) using Nessus Essentials on June 26, 2025, at 12:00 PM IST. The scan identified a total of 47 vulnerabilities, categorized by severity as follows:

- Critical: 1 vulnerability
- High: 1 vulnerability
- Medium: 4 vulnerabilities
- Low: 0 vulnerabilities
- Info: 41 vulnerabilities

The scan targeted the local machine to detect common vulnerabilities, including unsupported software versions, misconfigurations, and informational exposures. The single critical vulnerability requires immediate attention, while the high and medium issues should be addressed to enhance security. The provided screenshot (labeled ‘Scan$_{summary_1}27.0.0.1.png‘)isreferencedinAppendix$

# 2 Critical Vulnerabilities

The following critical vulnerability was identified during the scan and poses a significant risk that should be addressed immediately.

## 2.1 Oracle Database Unsupported Version Detection

- **Severity**: Critical
- **CVSS v3.0 Score**: 10.0*
- **Plugin ID**: 55786
- **Description**: The installed Oracle Database version is unsupported or end-of-life, exposing the system to known exploits and vulnerabilities due to lack of security patches.
- **Affected Component**: Oracle Database (version unspecified)
- **Mitigation**: Upgrade to a supported Oracle Database version (e.g., 19c or later) and apply the latest patches. Consult Oracles support documentation for upgrade instructions.

# 3 High-Severity Vulnerabilities

The following high-severity vulnerability was identified and should be prioritized for remediation.

### 3.1 Oracle TNS Listener Remote Poisoning

- **Severity**: High
- **CVSS v3.0 Score**: 7.3
- **Plugin ID**: 69552
- **Description**: A vulnerability in the Oracle TNS Listener allows remote attackers to poison the listener configuration, potentially leading to denial-of-service or unauthorized access.
- **Affected Component**: Oracle TNS Listener
- **Mitigation**: Apply the latest Oracle patch set update (PSU) for the TNS Listener. Restrict access to the listener port (default 1521) via firewall rules.

## 4 Medium-Severity Vulnerabilities

The following medium-severity vulnerabilities were identified and should be addressed to improve system security.

### 4.1 SSL Certificate Cannot Be Trusted

- **Severity**: Medium
- **CVSS v3.0 Score**: 6.5
- **Plugin ID**: 51192
- **Description**: The SSL certificate in use is untrusted or expired, potentially leading to man-in-the-middle attacks.
- **Affected Component**: Web server SSL configuration
- **Mitigation**: Replace the certificate with a valid one from a trusted Certificate Authority (e.g., Lets Encrypt) and ensure automatic renewal is configured.

### 4.2 SMB Signing Not Required

- **Severity**: Medium
- **CVSS v3.0 Score**: 5.3
- **Plugin ID**: 57608
- **Description**: SMB signing is not required, increasing the risk of man-in-the-middle attacks or session hijacking.
- **Affected Component**: SMB service
- **Mitigation**: Enable SMB signing in the system configuration (e.g., via Windows Group Policy or Linux SMB settings).

### 4.3 Oracle Application Express (Apex) CVE-2011-3525

- **Severity**: Medium
- **CVSS v3.0 Score**: 6.5*
- **Plugin ID**: 64712
- **Description**: A vulnerability in Oracle Application Express allows unauthorized access due to improper input validation (CVE-2011-3525).
- **Affected Component**: Oracle Apex
- **Mitigation**: Apply the Oracle Critical Patch Update (CPU) for October 2011 or upgrade to a patched version.

### 4.4 Oracle Application Express (Apex) CVE-2012-1708

- **Severity**: Medium
- **CVSS v3.0 Score**: 4.3*
- **Plugin ID**: 64713
- **Description**: A cross-site scripting (XSS) vulnerability in Oracle Apex (CVE-2012-1708) allows attackers to inject malicious scripts.
- **Affected Component**: Oracle Apex
- **Mitigation**: Apply the Oracle CPU for April 2012 or upgrade to a secured version.

## 5 Recommendations

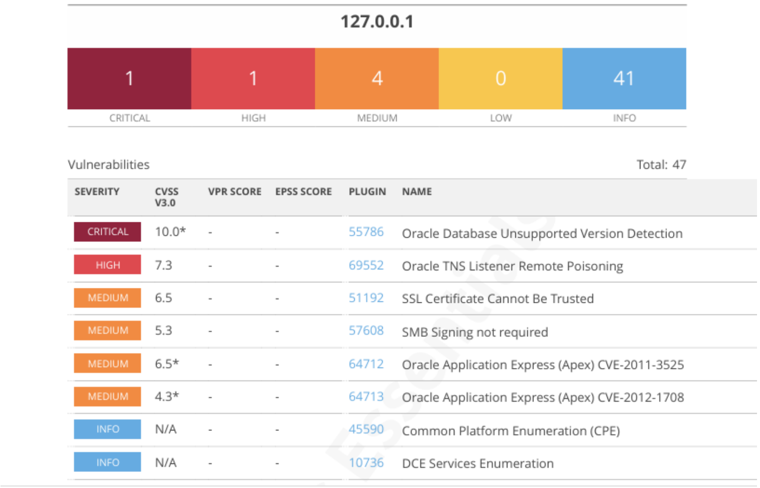
To secure the system and mitigate the identified vulnerabilities, the following actions are recommended:

- **Upgrade Software**: Update Oracle Database to a supported version and apply the latest patches to address the critical vulnerability.
- **Apply Patches**: Install Oracle patch set updates for TNS Listener and Apex to resolve high and medium-severity issues.
- **Certificate Management**: Replace the untrusted SSL certificate and configure automatic renewal to prevent future issues.
- **Enable Security Features**: Enforce SMB signing to mitigate man-in-the-middle risks.
- **Firewall Configuration**: Restrict access to critical ports (e.g., 1521 for TNS Listener) to reduce exposure.
- **Regular Scans**: Schedule periodic Nessus scans to monitor for new vulnerabilities, especially after software updates.

# 6 Appendix A: Screenshots

:

.



127.0.0.1

| 1 | 1 | 4 | 0 | 41 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities

Total: 47

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME |
|---|---|---|---|---|---|
| CRITICAL | 10.0* | - | - | 55786 | Oracle Database Unsupported Version Detection |
| HIGH | 7.3 | - | - | 69552 | Oracle TNS Listener Remote Poisoning |
| MEDIUM | 6.5 | - | - | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 5.3 | - | - | 57608 | SMB Signing not required |
| MEDIUM | 6.5* | - | - | 64712 | Oracle Application Express (Apex) CVE-2011-3525 |
| MEDIUM | 4.3* | - | - | 64713 | Oracle Application Express (Apex) CVE-2012-1708 |
| INFO | N/A | - | - | 45590 | Common Platform Enumeration (CPE) |
| INFO | N/A | - | - | 10736 | DCE Services Enumeration |