

VULNERABILITY ASSESSMENT REPORT

Tool Used: Tenable Nessus Essentials

Version: 10.11.2 Linux

Scanner: Local Scanner

Target: 127.0.0.1 (Localhost)

Scan Type: Basic Network Scan

Scan Duration: 41 Minutes

Date: February 15, 2026

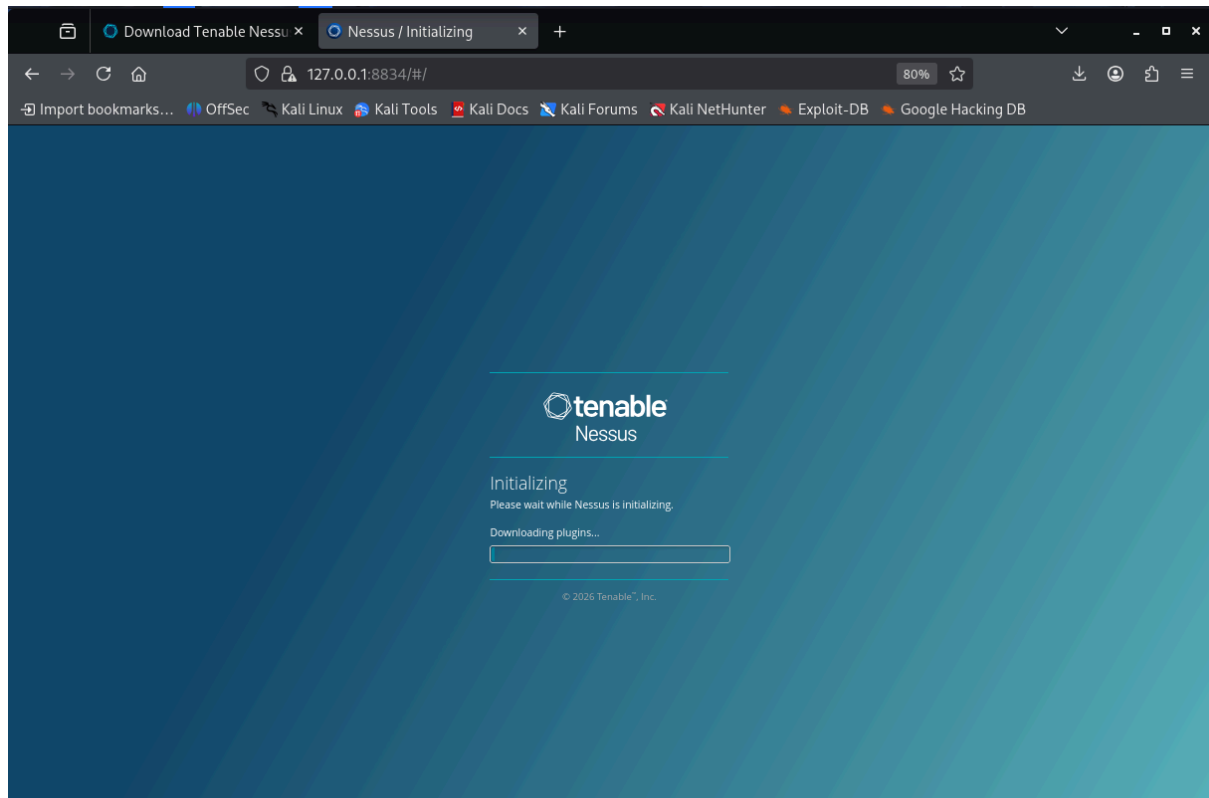
1. Installation & Service Verification

1.1 Nessus Installation

The Nessus package `Nessus-10.11.2-debian10_amd64.deb` was successfully installed using dpkg.

Screenshot Placement:

Insert screenshot:



Unique Identifying Clue:

Look for:

- "INSTALL PASSED"
- cryptographic self-tests (HMAC, SHA1, RSA, etc.)
- Message: *You can start Nessus Scanner by typing /bin/systemctl start nessusd.service*

This confirms successful installation.

1.2 Nessus Service Status Verification

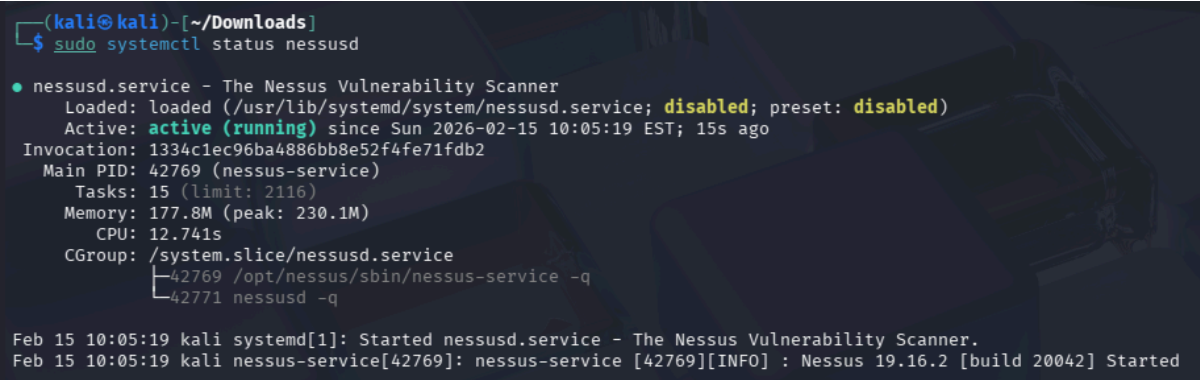
The Nessus service was verified using:

```
sudo systemctl status nessusd
```

Service status: **Active (running)**

Screenshot Placement:

Insert screenshot:



```
(kali@kali)-[~/Downloads]
$ sudo systemctl status nessusd

● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Sun 2026-02-15 10:05:19 EST; 15s ago
 Invocation: 1334c1ec96ba4886bb8e52f4fe71fdb2
    Main PID: 42769 (nessus-service)
       Tasks: 15 (limit: 2116)
    Memory: 177.8M (peak: 230.1M)
         CPU: 12.741s
    CGroup: /system.slice/nessusd.service
            └─42769 /opt/nessus/sbin/nessus-service -q
              └─42771 nessusd -q

Feb 15 10:05:19 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Feb 15 10:05:19 kali nessus-service[42769]: nessus-service [42769][INFO] : Nessus 19.16.2 [build 20042] Started
```

Unique Identifying Clue:

- Service name: `nessusd.service`
- Status: `Active (running)`
- Main PID visible

- Timestamp: Feb 15

2. Plugin Initialization & Updates

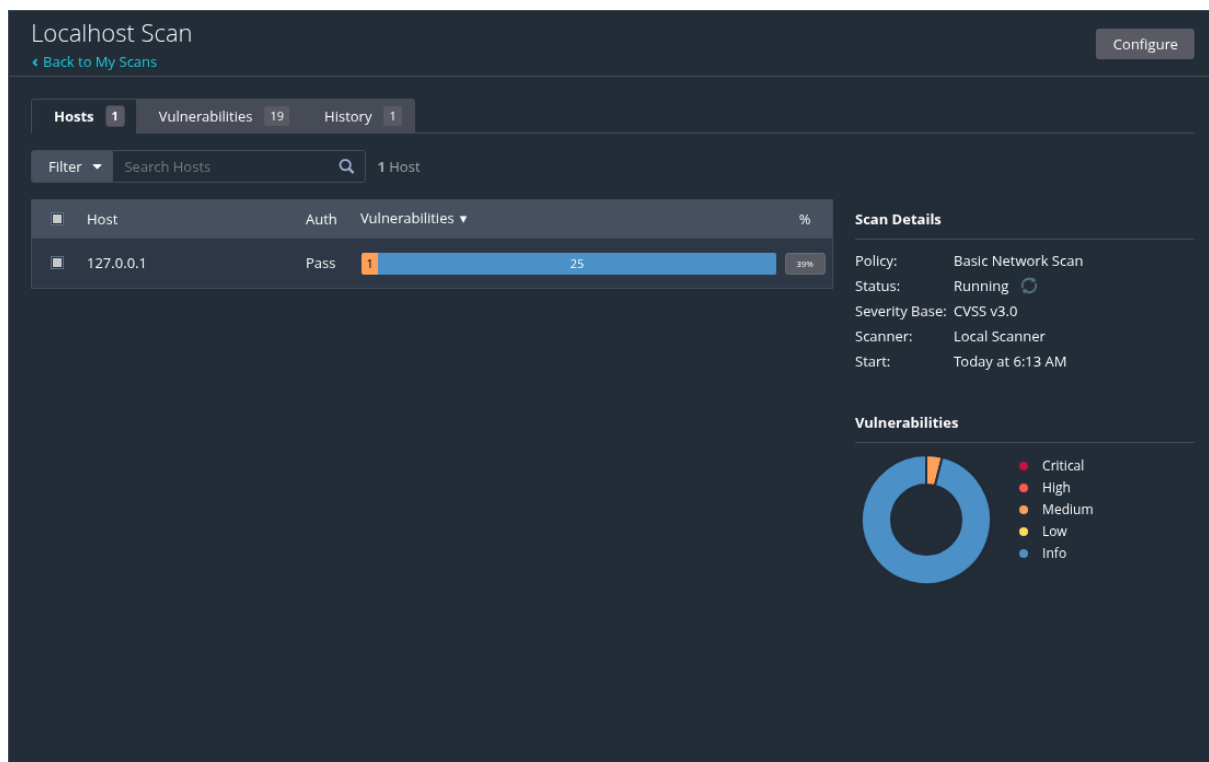
Initially, plugin downloads failed due to network issues. After resolving network/DNS configuration, plugins were successfully updated.

Final Status:

- Nessus Plugins: Complete
- Nessus Core Components: Complete

Screenshot Placement:

Insert screenshot:



Unique Identifying Clue:

- Shows "Nessus Plugins: Complete"
- Mentions copying templates version 202601121526

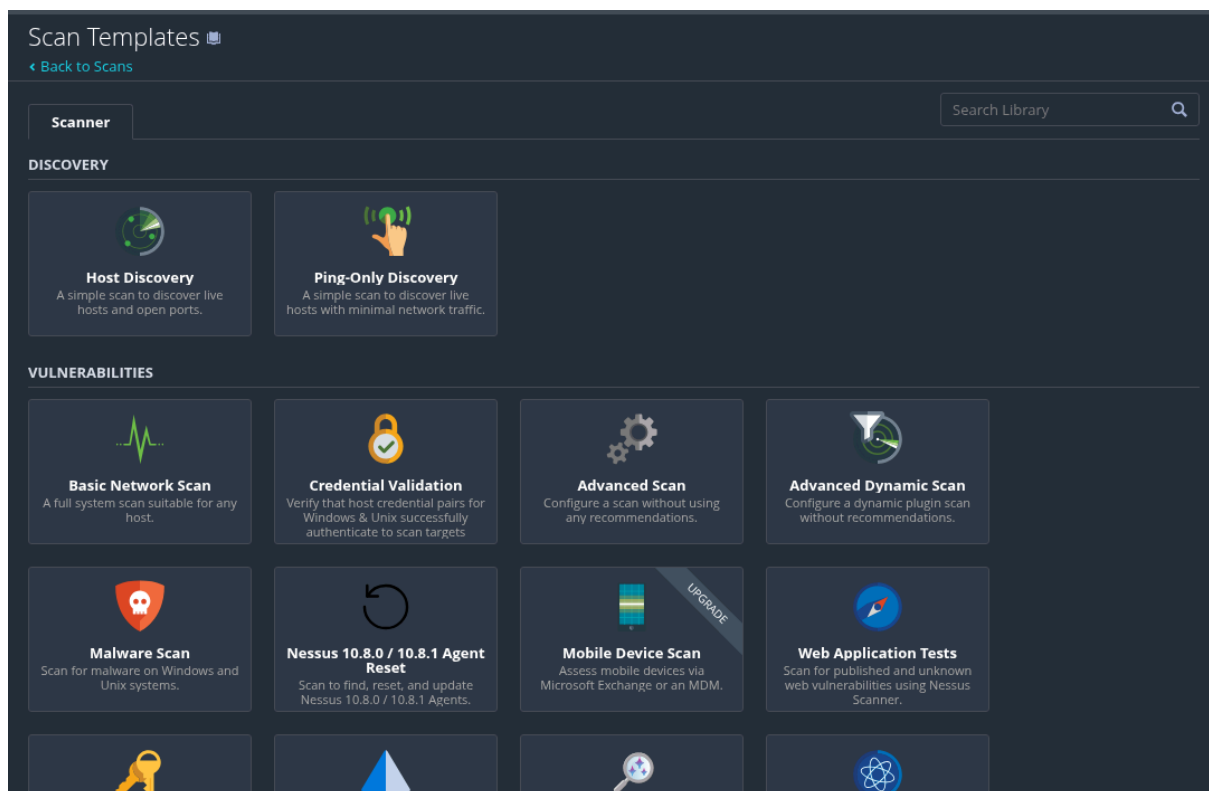
3. Dashboard & Scan Configuration

3.1 Scan Template Selection

Basic Network Scan template was selected.

Screenshot Placement:

Insert:



Unique Clue:

- Template name: Basic Network Scan
- Other templates visible: Malware Scan, Advanced Scan, etc.

3.2 Scan Configuration

Configured:

- Name: Localhost Scan
- Target: 127.0.0.1
- Folder: My Scans

Screenshot Placement:

Insert:

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Localhost Scan

Description: Testing Nessus

Folder: My Scans

Targets: 127.0.0.1

Upload Targets [Add File](#)

Save Cancel

Unique Clue:

- Target field contains: 127.0.0.1
 - Description: Testing Nessus
-

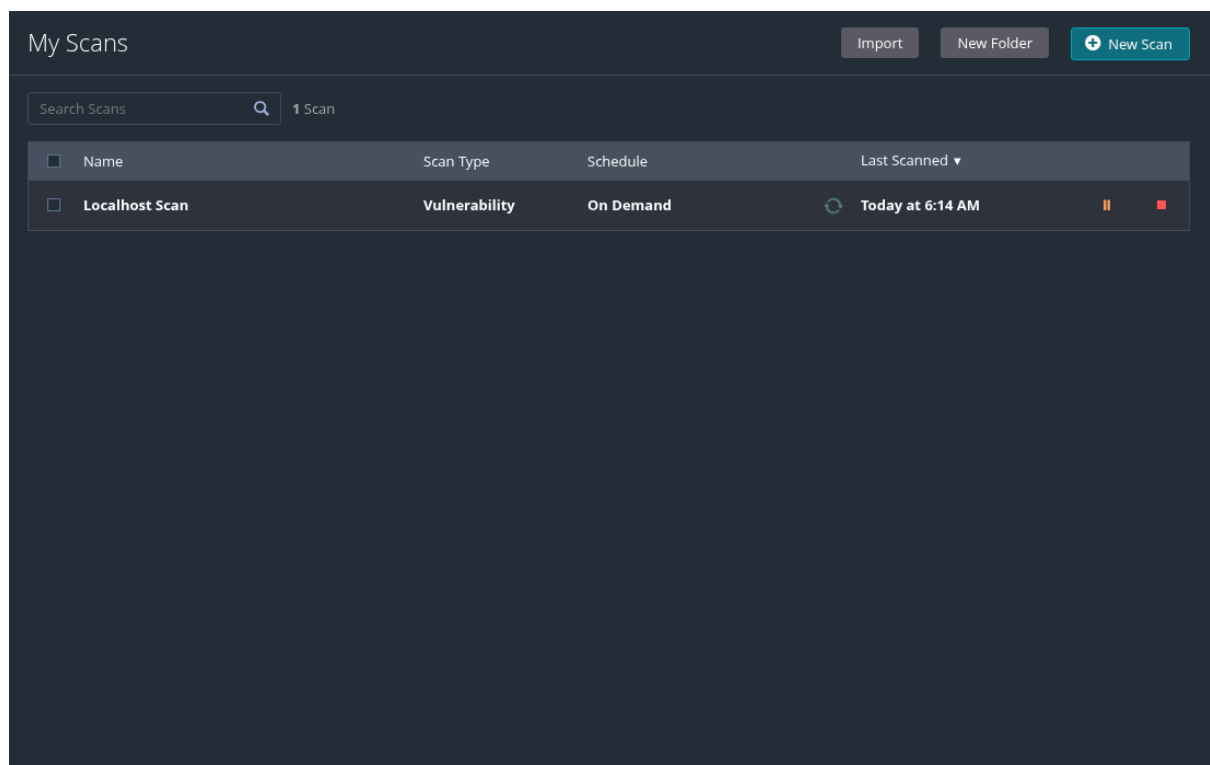
4. Scan Execution

Scan Status:

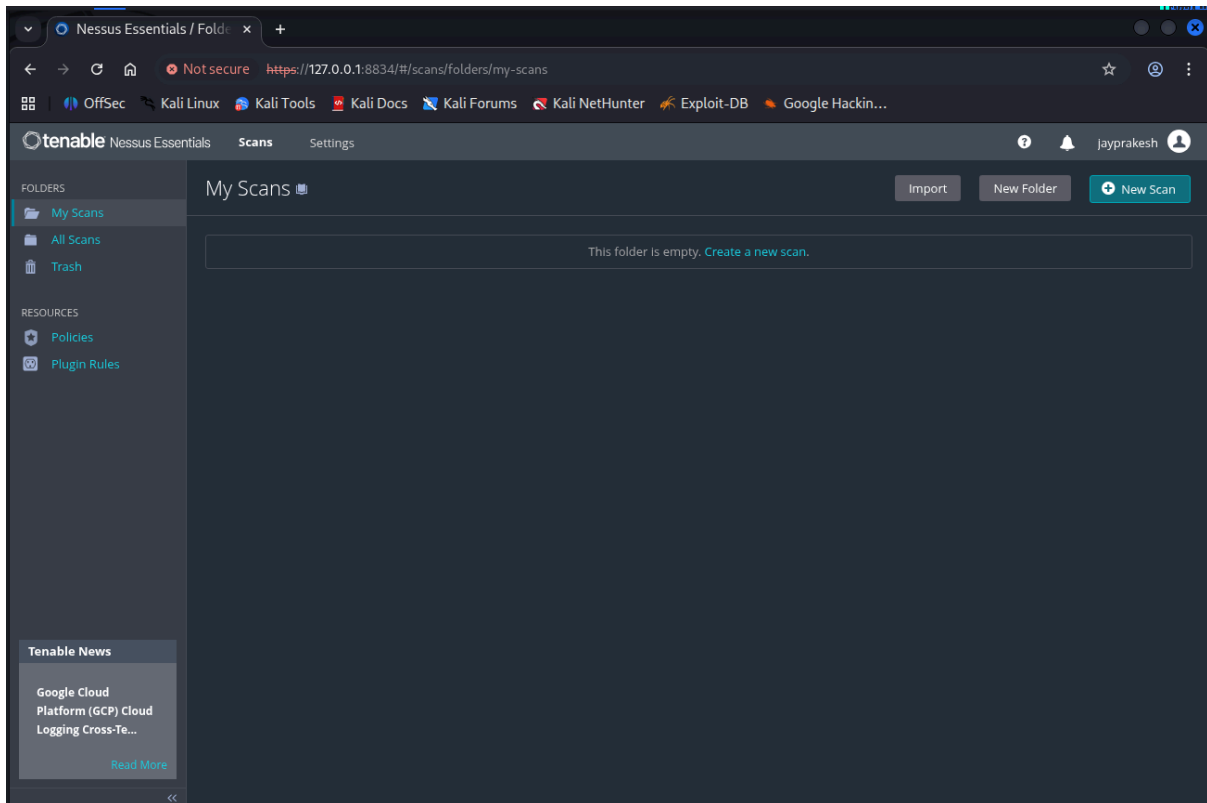
- Policy: Basic Network Scan
- Status: Completed
- Duration: 41 minutes
- Start Time: 6:13 AM
- End Time: 6:54 AM

Screenshot Placement:

Insert:



and then



Unique Clue:

- Elapsed: 41 minutes
- Scanner: Local Scanner
- Status: Completed

5. Scan Results Overview

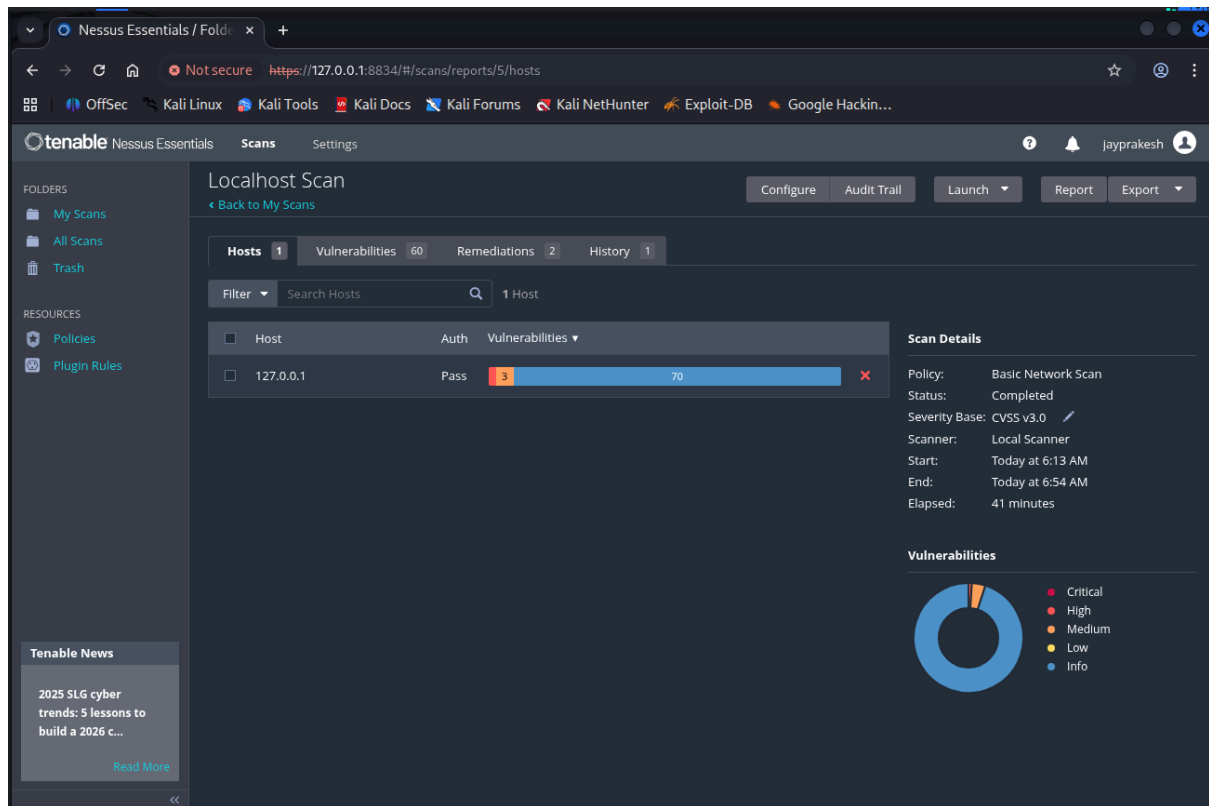
Total Vulnerabilities Detected: 60

Severity Distribution:

- High: 3
- Medium: 2
- Info: Remaining

Screenshot Placement:

Insert:



Unique Clue:

- Vulnerabilities count shows: 60
- Host: 127.0.0.1
- Donut severity chart visible

6. High Severity Vulnerability Analysis

Vulnerability Identified:

Python Library Brotli <= 1.1.0 DoS

Severity: HIGH
CVSS v3.0 Score: 7.5
CVE: CVE-2025-6176

Technical Details:

Installed Version: 1.1.0
Fixed Version: 1.2.0
Path:

/usr/lib/python3/dist-packages/Brotli-1.1.0.egg-info

Screenshot Placement:

Insert:

HIGH Python Library Brotli <= 1.1.0 DoS

Description

The detected version of the Brotli Python package, Brotli, is prior or equal to 1.1.0. It is, therefore, affected by a denial of service (DoS) vulnerability due to decompression.
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Brotli version 1.2.0 or later.

See Also

<https://github.com/advisories/GHSA-2qfp-q593-8484>

Output

Path : /usr/lib/python3/dist-packages/Brotli-1.1.0.egg-info
Installed version : 1.1.0
Fixed version : 1.2.0

To see debug logs, please visit individual host

Port ▲

Hosts

N/A

127.0.0.1

Plugin Details

Severity: High
ID: 274433
Version: 1.1
Type: local
Family: Misc.
Published: November 7, 2025
Modified: November 7, 2025

Risk Information

Exploit Prediction Scoring System (EPSS): 0.0004
Risk Factor: High
CVSS v3.0 Base Score: 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v2.0 Base Score: 7.8
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C
IAVM Severity: I

Vulnerability Information

CPE: cpe:/a:python:brotli
Patch Pub Date: October 30, 2025
Vulnerability Pub Date: October 30, 2025

Reference Information

IAVA: 2025-A-0813
CVE: CVE-2025-6176

Unique Clue:

- CVSS v3.0 Base Score: 7.5
- EPSS: 0.0004
- Shows "Upgrade to Brotli version 1.2.0 or later"

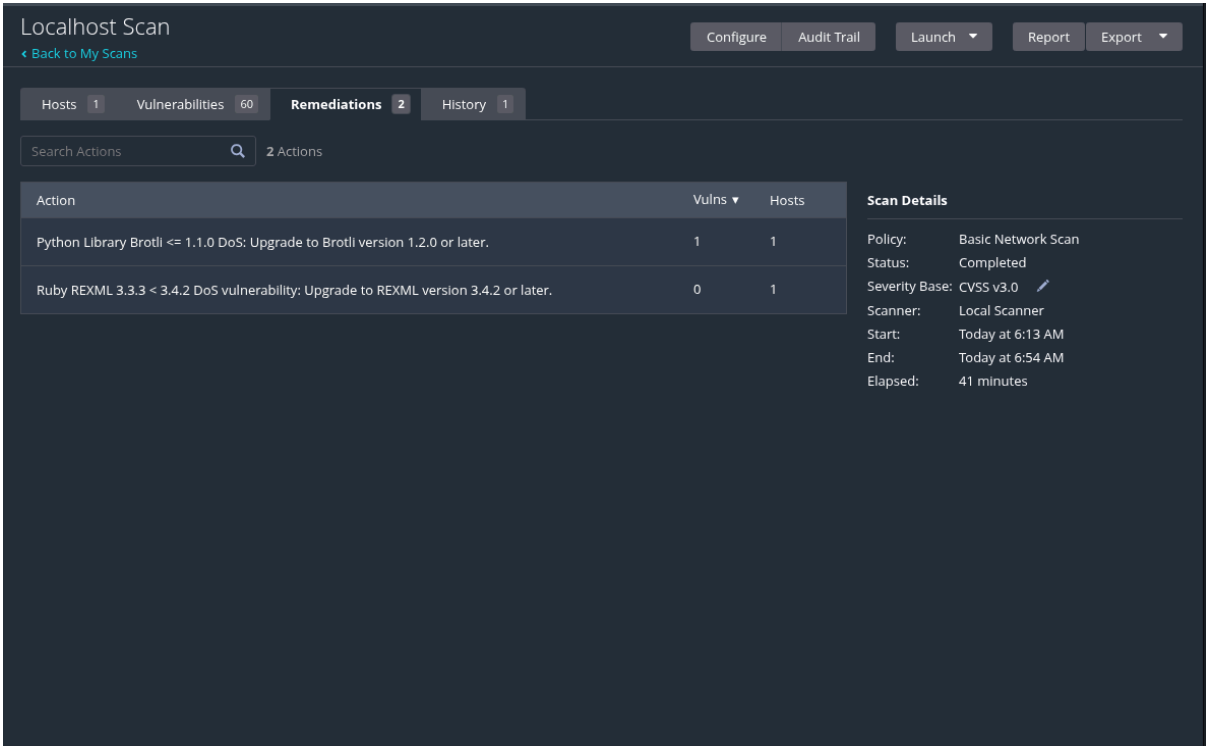
7. Remediation Summary

Two remediation actions identified:

1. Upgrade Brotli to 1.2.0+
2. Upgrade Ruby REXML to 3.4.2+

Screenshot Placement:

Insert:



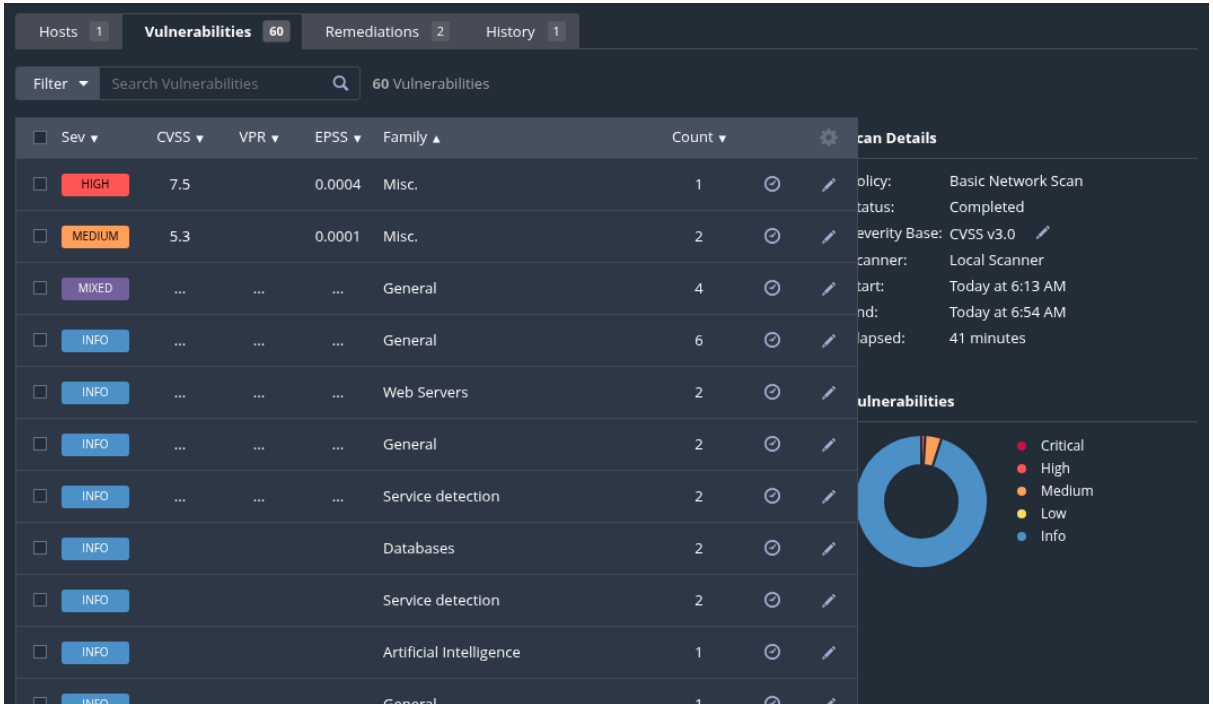
Unique Clue:

- Remediation tab selected
- Shows 2 Actions
- Mentions Brotli and REXML

8. Vulnerability Listings (Evidence Section)

These screenshots show categorized vulnerability listings.

Insert in this order:

1. 

The screenshot displays a vulnerability management dashboard. At the top, there are tabs for Hosts (1), Vulnerabilities (60), Remediations (2), and History (1). Below the tabs is a search bar labeled 'Search Vulnerabilities' and a count of '60 Vulnerabilities'. The main table lists vulnerabilities with columns for Severity (Sev), CVSS, VPR, EPSS, Family, and Count. The first two rows are highlighted: one with a HIGH severity (CVSS 7.5) and another with a MEDIUM severity (CVSS 5.3). The sidebar on the right shows 'Scan Details' including policy, status, severity base, scanner, start time, end time, and elapsed time. Below the details is a 'Vulnerabilities' section with a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (dark blue).

Sev	CVSS	VPR	EPSS	Family	Count
HIGH	7.5		0.0004	Misc.	1
MEDIUM	5.3		0.0001	Misc.	2
MIXED	General	4
INFO	General	6
INFO	Web Servers	2
INFO	General	2
INFO	Service detection	2
INFO	Databases	2
INFO	Service detection	2
INFO	Artificial Intelligence	1
INFO	General	1

2.

<input type="checkbox"/>	INFO	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	Misc.	1	🔄	✎

3.

<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	Settings	1	🔄	✎
<input type="checkbox"/>	INFO	Service detection	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	Port scanners	1	🔄	✎
<input type="checkbox"/>	INFO	Web Servers	1	🔄	✎
<input type="checkbox"/>	INFO	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	Artificial Intelligence	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	Misc.	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎
<input type="checkbox"/>	INFO	General	1	🔄	✎

<input type="checkbox"/>	INFO	Misc.	1	🕒	✎
<input type="checkbox"/>	INFO	Artificial Intelligence	1	🕒	✎
<input type="checkbox"/>	INFO	General	1	🕒	✎
<input type="checkbox"/>	INFO	Misc.	1	🕒	✎
<input type="checkbox"/>	INFO	Misc.	1	🕒	✎
<input type="checkbox"/>	INFO	General	1	🕒	✎
<input type="checkbox"/>	INFO	General	1	🕒	✎
<input type="checkbox"/>	INFO	Misc.	1	🕒	✎
<input type="checkbox"/>	INFO	Settings	1	🕒	✎
<input type="checkbox"/>	INFO	General	1	🕒	✎
<input type="checkbox"/>	INFO	General	1	🕒	✎
<input type="checkbox"/>	INFO	General	1	🕒	✎
<input type="checkbox"/>	INFO	Misc.	1	🕒	✎
<input type="checkbox"/>	INFO	Misc.	1	🕒	✎
<input type="checkbox"/>	INFO	Web Servers	1	🕒	✎

4.

Hosts1

Vulnerabilities60

Remediations2

History1

Filter

Search Vulnerabilities

60 Vulnerabilities

<input type="checkbox"/> Sev	CVSS	VPR	EPSS	Family	Count	
<input type="checkbox"/> INFO				Service detection	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> INFO				Settings	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> INFO				Settings	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> INFO				Misc.	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> INFO				General	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> INFO				Misc.	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> INFO				Misc.	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> INFO				General	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> INFO				Settings	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> INFO				Misc.	1	<input checked="" type="checkbox"/>

5.

Unique Clue for Each:

All contain:

- Severity column (INFO, MEDIUM, HIGH)
- CVSS column
- Family column
- Count column

Each screenshot scroll position differs — that proves they are separate captures.

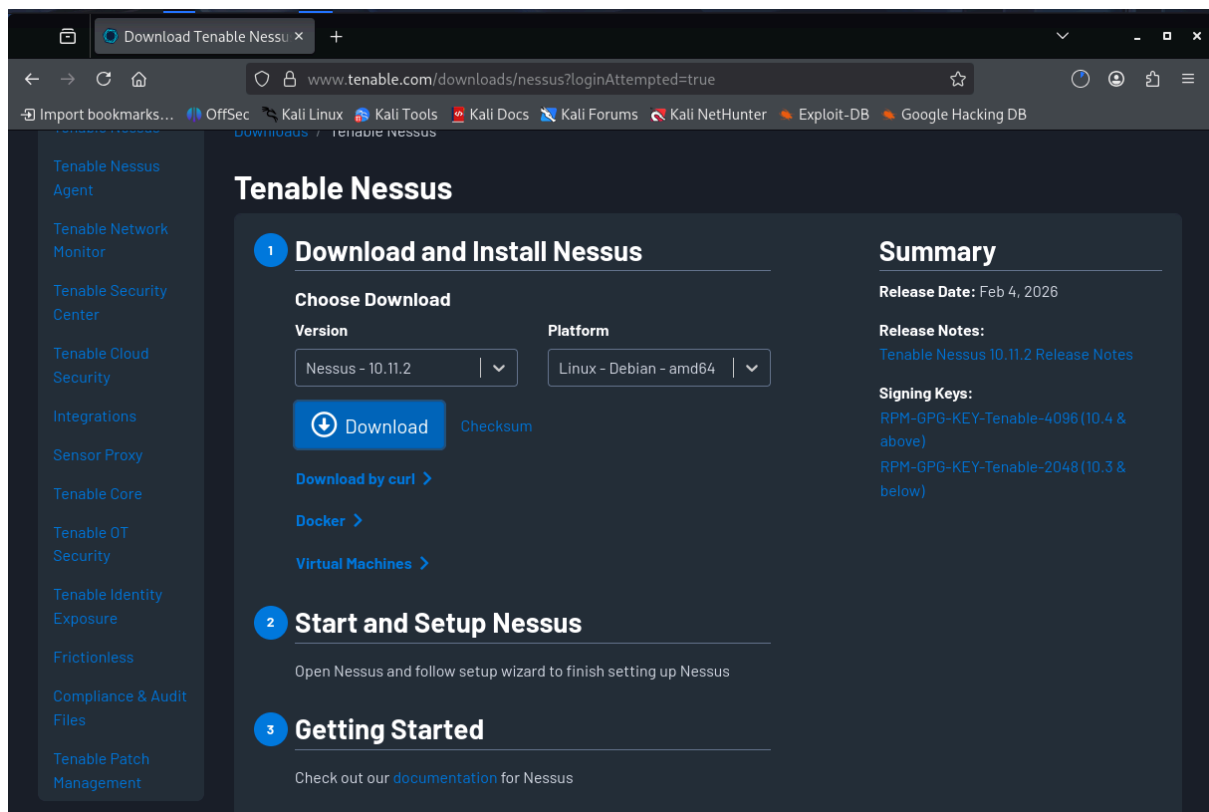
9. License & About Information

Nessus Essentials Version:
10.11.2 (#42) LINUX

License Expiration:
March 17, 2026

Screenshot Placement:

Insert:



Unique Clue:

- Licensed Hosts: 0 of 5 used
 - Activation Code visible
-

10. Conclusions

- Nessus was successfully installed and configured.
 - Plugins were updated after resolving network issues.
 - A full Basic Network Scan was conducted.
 - 60 vulnerabilities detected.
 - 3 High Severity vulnerabilities found.
 - Primary high-risk issue: Brotli library DoS vulnerability.
 - Immediate remediation recommended.
-

11. Recommendations

1. Upgrade Brotli to version 1.2.0+
2. Update Ruby REXML library
3. Regularly update Nessus plugins
4. Schedule weekly vulnerability scans
5. Enable automatic updates