

## Vulnerability Assessment Report

**Scan Summary - Tool Used:** OpenVAS (GVM 25.04.0) - **Scan Target:** 127.0.0.1 (Localhost)  
- **Scan Type:** Full and Fast - **Date of Scan:** June 26, 2025 - **Total Vulnerabilities Found:** 5 -  
High: 1 - Medium: 2 - Low: 2

---

### Top Vulnerabilities and Recommendations

#### 1. TLSv1.0 Protocol Supported

- **Severity:** High
- **Description:** The server supports the outdated and insecure TLS 1.0 protocol. This may allow attackers to downgrade secure connections and exploit known weaknesses.
- **CVE:** Not assigned
- **Affected Port:** 443/tcp
- **Fix:** Disable TLS 1.0 and TLS 1.1 in the server configuration. Ensure only TLS 1.2 and 1.3 are enabled.

#### 2. Apache HTTP TRACE Method Enabled

- **Severity:** Medium
- **Description:** The TRACE HTTP method is enabled on the Apache web server. It can be exploited in Cross-Site Tracing (XST) attacks.
- **CVE:** CVE-2004-2320
- **Affected Port:** 80/tcp
- **Fix:** Add `TraceEnable off` to the Apache configuration file and restart the service.

#### 3. SSH Server CBC Mode Ciphers Enabled

- **Severity:** Low
- **Description:** The SSH server supports CBC-mode ciphers which are vulnerable to plaintext recovery attacks.
- **CVE:** N/A
- **Affected Port:** 22/tcp

- **Fix:** Update sshd\_config to disable CBC ciphers and only allow CTR or GCM modes.
- 4. **Outdated Software Detected: OpenSSH**
  - **Severity:** Medium
  - **Description:** The version of OpenSSH installed has known vulnerabilities.
  - **Fix:** Update OpenSSH to the latest stable version.
- 5. **Service Banner Disclosure**
  - **Severity:** Low
  - **Description:** Some services disclose version information in banners, which can help attackers during reconnaissance.
  - **Fix:** Configure services to suppress version banners where possible.

---

## Remediation Plan

Vulnerability	Action Taken	Responsible Team	Deadline
TLS 1.0 Protocol Support	Disable TLS 1.0/1.1 in server config	System Admin	June 28, 2025
Apache TRACE Method Enabled	Modify Apache config to disable TRACE	DevOps	June 28, 2025
SSH CBC Mode Ciphers	Update sshd_config to remove CBC	System Admin	June 30, 2025
Outdated OpenSSH Version	Update OpenSSH to latest version	IT Security	July 1, 2025
Service Banner Disclosure	Suppress service banners	DevOps	July 2, 2025

---