**Vulnerability Report**

**Name:** Prasad Jadhav

**Vulnerability Title:** Operating System (OS) End of Life (EOL) Detection  
**Plugin ID:** 1.3.6.1.4.1.25623.1.0.103674  
**CVE ID:** *Not Applicable (EOL status, not a specific CVE)*  
**Host Scanned:** 192.168.1.163 (DC-2)  
**Tool Used:** OpenVAS  
**Scan Date:** May 11, 2025

**1. Description:** The scan detected that the operating system running on the target host is **Debian GNU/Linux 8**, which has reached **End of Life (EOL)**. This means it is no longer receiving security updates or patches from the vendor. Continued use of this unsupported OS version poses a high risk to system integrity and network security, as newly discovered vulnerabilities will remain unpatched.

**2. Risk Summary:**

* **Risk Factor:** Critical
* **CVSS v3.0 Base Score:** 10.0 (based on unpatched OS surface and critical exposure)
* **Attack Vector:** Network
* **Impact:**
  + No vendor support or security patches
  + Exposure to known and zero-day vulnerabilities
  + Increased risk of full system compromise
* **Exploitable Remotely:** Yes (if other vulnerable services are exposed)
* **Authentication Required:** No

**3. Affected Software/Services:**

* **Operating System:** Debian GNU/Linux
* **Detected Version:** 8
* **EOL Date:** June 30, 2020
* **CPE:** cpe:/o:debian:debian\_linux:8

**4. Remedies:**

* Migrate to a supported Debian release (e.g., Debian 11 "Bullseye" or Debian 12 "Bookworm").
* Reinstall or upgrade the system to a version that receives security patches and updates.
* Ensure that software and services running on the OS are compatible with newer versions before migration.

**5. Recommendations:**

* **Immediate replacement** of the affected OS with a supported version.
* **Inventory audit** of all systems in the network for EOL software.
* Establish a **lifecycle management policy** to track EOL software and schedule upgrades before support ends.
* Apply **network segmentation** and **access restrictions** to limit exposure of EOL systems until they are upgraded.

**6. References:**

* Debian Release Table - Wikipedia
* Debian Project - Release Info
* NIST CPE Database