# Operating System Patch Management RMF Compliance

**\*\*\* System Overview \*\*\***

**The system is a computer with the following specifications:**

* **Date: April 6th, 2025**
* **Time: 4:02 PM**
* **OS Name: kb322-18**
* **OS Version: Debian 6.1.129-1 (2025-03-06)**
* **Computer Name: kb322-18**
* **IP Address: 140.160.138.147**

**\*\*\* Patch Status Summary\*\*\***

**The following patches are pending updates:**

**1. Code/stable 1.99.0-1743632463 amd64 [upgradable from: 1.98.2-1741788907]**

**There is no information available about the relevance of this patch to security.**

**\*\*\* Compliance with RMF Controls\*\*\***

**To ensure compliance with the Risk Management Framework (RMF), we recommend:**

* **Flaw remediation in place by installing the pending update as soon as possible.**
* **Identification, reporting, and corrective action to monitor and report any vulnerabilities.**
* **Configuration management to track changes to system configurations and ensure consistency.**
* **Vulnerability checks to regularly scan for new vulnerabilities.**

**\*\*\* Recommended next steps\*\*\***

**The recommended next steps are:**

**1. Review and assess updates to determine the relevance of the pending patch to security.**
**2. Scheduling patch deployments to install the update as soon as possible.**
**3. Guidance for Update documentation to track changes to system configurations and ensure consistency.**

**\*\*\* Risk Assessment\*\*\***

**There is currently no information available about potential vulnerabilities, but the pending patch may address a known vulnerability. If installed promptly, this should mitigate any risk associated with the vulnerability. The potential impact level of this vulnerability is unknown, and further assessment would be required after installation of the patch.**