## Operating System Patch Management RMF Compliance

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

The system being monitored is a computer with the following specifications:

Date: 04-06-2025

Time: 16:02:09

OS Name: kb322-18

OS Version: #1 SMP PREEMPT\_DYNAMIC 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 and can be applied to bring the system up to date:

\* code/stable 1.99.0-1743632463 amd64

\* ure/stable-security 4:7.4.7-1+deb12u6 amd64

\* git-man/stable-security 1:2.39.5-0+deb12u2 all

\* git/stable-security 1:2.39.5-0+deb12u2 amd64

These patches are related to security and can help protect the system against potential vulnerabilities.

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

To ensure compliance, it is recommended that:

\* The updates be reviewed and assessed for their impact on the system.

\* A corrective action plan be put in place to address any identified vulnerabilities or weaknesses.

\* Configuration management practices be followed to ensure that the system is properly secured and up to date.

\* Vulnerability checks be conducted regularly to identify potential security risks.

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

The recommended next steps are:

\* Review and assess the updates for their impact on the system.

\* Schedule patch deployments, if necessary.

\* Document the update process in a way that makes it easy to track and manage future patches.

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

Based on the information provided, there is currently no indication of any pending security updates that could pose a risk to the system. However, regular vulnerability checks should be conducted to ensure that this remains the case.