Operating System Patch Management RMF Compliance

***** System Overview *****
Date: 04-04-2025
Time: 12:23:42
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 system is currently running an outdated version of the operating system, with the latest available patch being code/stable 1.99.0-1743632463 amd64. This patch addresses several security vulnerabilities.

Specifically, there are pending patches for the following systems:

*** Loggrove: A vulnerability classified as problematic has been found in this system, which could allow attackers to launch an attack remotely.**
*** Opcenter Execution Discrete, Opcenter Execution Foundation, Opcenter Execution Process, Opcenter Intelligence, Opcenter Quality, Opcenter RD&L, SIMATIC IT LMS, SIMATIC IT Production Suite, SIMATIC Notifier Server for Windows, SIMATIC PCS neo, SIMATIC STEP 7 (TIA Portal) V15, SIMATIC STEP 7 (TIA Portal) V16, SIMOCODE ES V15.1, SIMOCODE ES V16, Soft Starter ES V15.1, and Soft Starter ES V16: Several critical vulnerabilities have been identified in these systems, which could allow attackers to launch a partial remote denial-of-service or leak random information from the remote service.**

***** Compliance with RMF Controls *****
The current patch management process does not appear to be fully compliant with recommended controls. Specifically:

*** Flaw remediation is currently not in place.**
*** Identification, reporting, and corrective action are not clearly established.**
*** Configuration management is missing.**
*** Vulnerability checks are not being performed regularly.**

***** Recommended next steps *****
We recommend reviewing and assessing the available updates to ensure they address any newly discovered vulnerabilities.

After review and assessment, we should schedule patch deployments to apply the necessary updates to the system.

Additionally, it would be beneficial to establish a clear update documentation process to track and record all changes made to the system.

***** Risk Assessment *****
The potential risk associated with this system is moderate. The identified vulnerabilities pose a significant threat to the security of the system, which could lead to data breaches or disruptions to critical services.

To mitigate this risk, we should prioritize applying the recommended patches as soon as possible and establish a regular vulnerability check process to identify any newly

discovered issues before they can be exploited.