Operating System Patch Management RMF Compliance

***** System Overview *****

The system being patched 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 *****

There is one pending patch:
code/stable 1.99.0-1743632463 amd64 [upgradable from: 1.98.2-1741788907]

This patch is related to security and addresses a potential vulnerability in the system.

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

For flaw remediation, it is recommended that administrators review the list of affected products for this patch:
- Contact Manager App
- Loggrove
- 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, Soft Starter ES V16

For identification, reporting, and corrective action, it is recommended that administrators consult the CVE information for this patch to understand the vulnerability being addressed.

For configuration management, ensure that all configuration changes are documented and accounted for during the patch deployment process.

For vulnerability checks, run regular vulnerability scans on the system after applying the patch to ensure that the vulnerability has been fully addressed.

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

- Provide a review of the pending updates
- Scheduling patch deployments if necessary
- Guidance for update documentation

***** Risk Assessment *****

Since there is only one pending security patch, the potential risk associated with this patch is moderate. The impact level could be significant if left unaddressed. To mitigate this risk, ensure that the patch is applied in a timely manner and that regular vulnerability checks are performed after deployment to confirm that the system is fully

secured.