Operating System Patch Management RMF Compliance

Created April 27, 2025 at 15:55:13

System Overview

The systems in the network have received software updates to enhance security and stability.

Patch Status Summary

There are several systems with pending updates, including:

- Linux-image-amd64: Updated from version 6.1.129-1 to 6.1.135-1.
- perl-modules-5.36: Updated from version 5.36.0-7+deb12u1 to 5.36.0-7+deb12u2 (all).
- gir1.2-javascriptcoregtk-4.0, gir1.2-webkit2-4.0, libjavascriptcoregtk-4.0-18, and libwebkit2gtk-4.0: Updated from version 2.48.0-1~deb12u1 to 2.48.1-2~deb12u1 (all).

These updates are available for immediate installation.

Compliance with RMF Controls

In order to meet the requirements of the Risk Management Framework (RMF), it is essential to identify and remediate vulnerabilities that could pose a risk to the system.

- **Flaw Remediation:** The systems should be updated as soon as possible.
- **Identification, Reporting / Corrective Action:** Identify potential risks and report them to management. Perform corrective actions, such as updating software or patching vulnerabilities, in a timely manner.
- **Configuration Management:** Ensure that configuration settings are properly documented and updated regularly.
- **Vulnerability Checks:** Regularly check the systems for known vulnerabilities and address any issues promptly.

Recommended next steps

The first step is to Review and Assess Updates to determine if they align with organizational requirements and identify potential risks. Next, Schedule patch deployments for the pending updates to ensure that the systems are brought up-to-date in a timely manner. Finally, update documentation to reflect any changes or additions made to system configurations.

Risk Assessment

The current patches address some of the identified vulnerabilities; however, due to the nature of the updates and their availability, there is still a risk involved.

- **Potential Risk:** The potential risk is that the systems may not receive necessary security patches in a timely manner, leaving them vulnerable to attacks.
- **Impact Level:** The impact level could be significant if the vulnerability were to be exploited, potentially causing system downtime or data breaches.
- **Mitigation Plan:** To mitigate this risk, the organization should prioritize patching these updates as soon as possible.