Operating System Patch Management RMF Compliance

Created May 14, 2025 at 04:37:56

System Overview

The Debian GNU/Linux 12 (bookworm) operating system is currently running on the system, with an OS version of #1 SMP PREEMPT_DYNAMIC Debian 6.1.128-1 (2025-02-07). The system has a computer name of "debian-12" and an IP address of "172.24.24.12".

Patch Status Summary

The following patches are available for installation:

* base-files/stable: Update to version 12.4+deb12u10 (fixes security vulnerabilities)

* dns-root-data/stable: Update to version 2024071801~deb12u1 (improves DNS security)

* firefox-esr/stable-security: Update to version 128.10.0esr-1~deb12u1 (patches security vulnerabilities in Firefox)

* fonts-opensymbol/stable-security: Update to version 4:102.12+LibO7.4.7-1+deb12u8 (fixes font-related security issues)

* ghostscript/stable-security: Update to version 10.0.0~dfsg-11+deb12u7 (patched security vulnerabilities in Ghostscript)

* gir1.2-javascriptcoregtk-4.0/stable-security: Update to version 2.48.1-2~deb12u1 (fixes security vulnerabilities in JavaScriptCore)

* gir1.2-javascriptcoregtk-4.1/stable-security: Update to version 2.48.1-2~deb12u1 (fixes security vulnerabilities in JavaScriptCore)

* gir1.2-webkit2-4.0/stable-security: Update to version 2.48.1-2~deb12u1 (patched security vulnerabilities in WebKit)

* gir1.2-webkit2-4.1/stable-security: Update to version 2.48.1-2~deb12u1 (fixes security vulnerabilities in WebKit)

* libc-bin/stable: Update to version 2.36-9+deb12u10 (fixes library-related security issues)

* libc-l10n/stable: Update to version 2.36-9+deb12u10 (improves locale support)

* libc6/stable: Update to version 2.36-9+deb12u10 (fixes library-related security issues)

* libcurl3-gnutls/stable: Update to version 7.88.1-10+deb12u12 (patches security vulnerabilities in cURL)

* libcurl4/stable: Update to version 7.88.1-10+deb12u12 (fixes security vulnerabilities in cURL)

* libfreetype6/stable-security: Update to version 2.12.1+dfsg-5+deb12u4 (fixes font-related security issues)

* libgs-common/stable-security: Update to version 10.0.0~dfsg-11+deb12u7 (patched security vulnerabilities in Ghostscript)

* libgs10-common/stable-security: Update to version 10.0.0~dfsg-11+deb12u7 (fixes security vulnerabilities in Ghostscript)

* libgs10/stable-security: Update to version 10.0.0~dfsg-11+deb12u7 (patched security vulnerabilities in Ghostscript)

* libjavascriptcoregtk-4.0-18/stable-security: Update to version 2.48.1-2~deb12u1 (fixes security vulnerabilities in JavaScriptCore)

* libjavascriptcoregtk-4.1/stable-security: Update to version 2.48.1-2~deb12u1 (fixes security vulnerabilities in JavaScriptCore)

* libjavascriptcoregtk-6.0-1/stable-security: Update to version 2.48.1-2~deb12u1 (fixes security vulnerabilities in JavaScriptCore)

* liblzma5/stable-security: Update to version 5.4.1-1 (fixes compression-related security issues)

* libnss-myhostname/stable: Update to version 252.36-1~deb12u1 (improves hostname management)

* libnss-systemd/stable: Update to version 252.36-1~deb12u1 (fixes systemd-related security issues)

* libopenh264-7/stable: Update to version 2.3.1+dfsg-3+deb12u2 (patched security vulnerabilities in OpenH264)

* libpam-systemd/stable: Update to version 252.36-1~deb12u1 (fixes systemd-related security issues)

* libperl5.36/stable-security: Update to version 5.36.0-7+deb12u2 (fixes security vulnerabilities in Perl)

* librabbitmq4/stable: Update to version 0.11.0-1+deb12u1 (patched security vulnerabilities in RabbitMQ)

* libreoffice-base-core/stable-security: Update to version 4:7.4.7-1+deb12u8 (fixes security vulnerabilities in LibreOffice)

* libreoffice-calc/stable-security: Update to version 4:7.4.7-1+deb12u8 (patched security vulnerabilities in LibreOffice Calc)

* libreoffice-common/stable-security: Update to version 4:7.4.7-1+deb12u8 (fixes security vulnerabilities in LibreOffice)

* libreoffice-core/stable-security: Update to version 4:7.4.7-1+deb12u8 (patched security vulnerabilities in LibreOffice)

* libreoffice-draw/stable-security: Update to version 4:7.4.7-1+deb12u8 (fixes security vulnerabilities in LibreOffice Draw)

* libreoffice-gnome/stable-security: Update to version 4:7.4.7-1+deb12u8 (patched security vulnerabilities in LibreOffice Gnome)

* libreoffice-gtk3/stable-security: Update to version 4:7.4.7-1+deb12u8 (fixes security vulnerabilities in LibreOffice GTK3)

* libreoffice-help-common/stable-security: Update to version 4:7.4.7-1+deb12u8 (fixes security vulnerabilities in LibreOffice Help)

* libreoffice-help-en-us/stable-security: Update to version 4:7.4.7-1+deb12u8 (patched security vulnerabilities in LibreOffice Help En-US)

* libreoffice-impress/stable-security: Update to version 4:7.4.7-1+deb12u8 (fixes security vulnerabilities in LibreOffice Impress)

* libreoffice-math/stable-security: Update to version 4:7.4.7-1+deb12u8 (patched security vulnerabilities in LibreOffice Math)

* libreoffice-style-colibre/stable-security: Update to version 4:7.4.7-1+deb12u8 (fixes security vulnerabilities in LibreOffice Style Colibre)

* libreoffice-style-elementary/stable-security: Update to version 4:7.4.7-1+deb12u8 (patched security vulnerabilities in LibreOffice Style Elementary)

* libreoffice-writer/stable-security: Update to version 4:7.4.7-1+deb12u8 (fixes security vulnerabilities in LibreOffice Writer)

Compliance with RMF Controls

To ensure compliance with the RMF controls, it is recommended to apply all available patches and updates.

* For flaw remediation, review the provided patch information and follow the installation instructions.

* For identification, reporting, and corrective action, report any issues or concerns to the IT department or management team.

* For configuration management, ensure that all system configurations are up-to-date and compliant with the recommended settings.

* For vulnerability checks, run regular vulnerability scans using a trusted tool or service.

Recommended next steps

1. Review and assess the available updates.

2. Schedule patch deployments if necessary.

3. Update documentation to reflect any changes made during patching.

Risk Assessment

The system is currently vulnerable to security risks due to outdated software components. The patches available provide a solution to these vulnerabilities, which can help prevent potential security breaches.

However, it is essential to note that some of the updates may require significant system downtime or configuration changes. It is recommended to schedule these deployments during off-peak hours to minimize disruptions.

In summary, this report provides an overview of the current patch status on the Debian GNU/Linux 12 (bookworm) system and recommends taking proactive steps to ensure compliance with the RMF controls. By applying available patches and updates, the organization can reduce its exposure to security risks and maintain a secure IT environment.