

RMF Report for Operating System Patch Management

****Vulnerability Patch Management Report****

****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 current patch status summary indicates that there is ****1 pending update****, with a code version of 1.99.0-1743632463 amd64, which is upgradable from the previous version 1.98.2-1741788907. The security relevance of this update has not been determined at this time.

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

*** **Flaw Remediation:****

No information on flaw remediation was found for this system.

*** **Configuration Settings:****

No information on configuration settings were found for this system.

*** **Vulnerability Checks:****

No information on vulnerability checks were found for this system.

****Recommended Next Steps:****

1. Apply the pending update to address any potential vulnerabilities.
2. Review and verify that all necessary configurations are up-to-date and secure.
3. Conduct a thorough vulnerability scan to identify any open or remediated issues.

****Risk Assessment:****

Due to the presence of a pending update, there is an increased risk of exposure to potential security vulnerabilities. It is recommended that this system be patched as soon as possible to mitigate these risks.

Please note that without further information on the patch's details and any affected components, it is challenging to provide a more detailed risk assessment.