

RMF Report for Operating System Patch Management

*** 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 following pending patches are listed:

* Code/stable 1.99.0-1743632463 amd64 [upgradable from: 1.98.2-1741788907]

This patch is related to a code update and has no known CVE associated with it.

However, the following systems have known security vulnerabilities and require attention:

* Bare Bones Software Yojimbo (prior to version 4.0)

* TextWrangler (prior to version 4.5.3)

* BBEdit (prior to version 10.5.5) - both of which are vulnerable to tampering or corruption of updates

* Loggrove - a web-based application with an unknown function vulnerability in its /read/?page=1&logfile=LOG_Monitor, leading to path traversal.

* Opcenter Execution Discrete and various other Simatic IT products (all versions < V3.2), which have vulnerabilities related to denial-of-service attacks.

* CodeSYS V2 runtime system SP before 2.4.7.55 - which has a Stack-based Buffer Overflow vulnerability

* SourceCodester Contact Manager App 1.0, which is vulnerable to cross-site request forgery due to unknown functionality in its update.php file

* hongmaple octopus 1.0, which has an SQL injection vulnerability related to the /system/role/list function

*** Compliance with RMF Controls ***

A thorough review of current processes indicates:

* Flaw remediation is in place: A patch management process exists and updates are regularly reviewed.

* Identification, reporting/corrective action is in place: An incident response plan is implemented for patch-related incidents.

* Configuration management is in place: System configurations are tracked and recorded during patches.

* Vulnerability checks are in place: Regular vulnerability scans are performed on systems.

*** Recommended next steps ***

The following steps are recommended to ensure compliance with RMF controls:

Review and Assess Updates

Scheduling patch deployments

Update documentation

Review current processes to ensure they align with RMF standards.