March 12, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that SAP published security advisories to address vulnerabilities in multiple products. Included were critical updates for the following:

- SAP Build Apps – versions prior to 4.9.145
- SAP NetWeaver AS Java (Administrator Log Viewer plug-in) – version 7.50

Technical Details
This post shares information on Security Notes that remediates vulnerabilities discovered in SAP products. SAP strongly recommends that the customer applies patches on priority to protect their SAP landscape.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2019-10744 CVE-2024-22127 CVE-2023-39439 CVE-2023-50164 CVE-2024-27902] CVE-2024-25644 CVE-2024-25645 CVE-2024-28163 CVE-2024-22133 CVE-2024-27900
- SAP Security Patch Day - March 2024