

Overall rating: Critical



This notification is intended as an informational bulletin 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 BTP Security Services Integration Library @sap/xssec – versions prior to 3.6.0
- SAP Application Router Library @sap/approuter – version 14.4.2
- SAP Edge Integration Cell – versions 8.9.13 and later

Technical Details

Escalation of Privileges in applications developed through SAP Business Application Studio, SAP Web IDE Full-Stack and SAP Web IDE for SAP HANA

Library-@sap/xssec, Versions < 3.6.0

Library-@sap/approuter, Versions –14.4.2

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify [VRM](#) with any questions or concerns you may have.

References

- CVE-2023-49583, CVE-2023-50422, CVE-2023-50423, CVE-2023-50424, CVE-2024-21737, CVE-2023-44487, CVE-2024-22125, CVE-2024-21735
- [SAP Security Patch Day ** – January 2024](#)