Overall rating: Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

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

- SAP Business One – version 10.0

Technical Details

SAP CommonCryptoLib does not perform necessary authentication checks, which may result in missing or wrong authorization checks for an authenticated user, resulting in escalation of privileges. Depending on the application and the level of privileges acquired, an attacker could abuse functionality restricted to a particular user group as well as read, modify or delete restricted data.

This vulnerability is rated as a **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-2023-40309, CVE-2023-31403, CVE-2023-42477
- SAP Security Patch Day – November 2023

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts