Overall rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware the July SAP Security Patch Day 2023, SAP released 16 (+2 Updates) security corrections, including fixes for its flagship products such as SAP NetWeaver AS for ABAP and ABAP Platform, SAP NetWeaver for Java, and SAP Business Object Business Intelligence Platform.

Technical Details

Security updates for the browser control Google Chromium delivered with SAP Business Client.
Product-SAP Business Client, Versions -6.5, 7.0, 7.70.

Another critical vulnerability is the OS command injection vulnerability in SAP ECC and SAP S/4HANA (IS-OI (listed as CVE-2023-36922).

Another vulnerability fixed with SAP Note 3331376 (listed as CVE-2023-33987) is rated with CVSS 8.6 at Product- SAP Web Dispatcher

These vulnerabilities are rated as an overall **High** Severity Threat. Please perform mitigating actions, as required.

.

Action Required

- Locate the device(s) or application(s) and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required within 14 Days of receiving this notification.

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

References

- Digital Library (sap.com)
- CVE-2023-36922 CVE-2023-33989 CVE-2023-33987 CVE-2023-33991 CVE-2023-33990 CVE-2023-35871 CVE-2023-36925 CVE-2023-36921 CVE-2023-35873 CVE-2023-35872