May 14, 2024

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

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

- SAP CX Commerce – version HY_COM 2205
- SAP NetWeaver Application Server ABAP and ABAP Platform – multiple versions

Technical Details

An unauthenticated attacker can upload a malicious file to the server which when accessed by a victim can allow an attacker to completely compromise system.

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-2024-33006 CVE-2024-28165 CVE-2024-32730 CVE-2024-34687 CVE-2024-32733 CVE-2024-33002 CVE-2024-32731 CVE-2024-33008 CVE-2024-33004 CVE-2024-33009
- SAP Security Patch Day - May 2024