Security Advisory 2023-019

Several Critical Vulnerabilities in SAP Products

March 15, 2023 — v1.0

TLP:CLEAR

History:

- *15/03/2023 — v1.0 – Initial publication*

Summary

On March 14, 2023, SAP released 19 patches for various products [1] which contain five critical severity fixes for SAP Business Objects Business Intelligence Platform (CMC) and SAP NetWeaver [2]:

- Improper Access Control in SAP NetWeaver AS for Java (CVE-2023-23857)
- Code Injection vulnerability in SAP Business Objects Business Intelligence Platform (CMC) (CVE-2023-25616)
- OS command execution vulnerability in SAP Business Objects Business Intelligence Platform (Adaptive Job Server) (CVE-2023-25617)
- Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform (CVE-2023-27269)
- Directory Traversal vulnerability in SAP ERP and S4HANA (SAPRSBRO Program) (CVE-2023-27500)

Due to its high global market share, SAP products are a valuable target for threat actors and criminals. Therefore, CERT-EU recommends applying the issued patches as soon as possible.

Technical Details

- CVE-2023-23857: An information disclosure, data manipulation, and DoS flaw that allows an unauthenticated attacker to perform unauthorised operations by attaching to an open interface and accessing services via the directory API.
- CVE-2023-25616: A code injection vulnerability allowing an attacker to access resources only available to privileged users.
- CVE-2023-25617: A command execution vulnerability allowing a remote attacker under certain conditions to execute arbitrary commands on the operating system.
- CVE-2023-27269: A directory traversal problem that allows a non-admin user to overwrite system files.
- CVE-2023-27500: A directory traversal problem allowing an attacker to overwrite system files and causing damage to the vulnerable endpoint.

Affected Products

- CVE-2023-27269: SAP NetWeaver Application Server for ABAP, versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, and 791.
- CVE-2023-25616: SAP Business Intelligence Platform, versions 420 and 430.
- CVE-2023-25617: SAP Business Intelligence Platform, versions 420 and 430.
- CVE-2023-23857: SAP NetWeaver AS for Java, version 7.50.
- CVE-2023-27500: SAP NetWeaver Application Server for ABAP, versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757.

Recommendations

CERT-EU firmly recommends applying the security fixes for these critical vulnerabilities. Additionally, applying the other 14 patches is also recommended.

References

[1] https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

[2] https://www.bleepingcomputer.com/news/security/sap-releases-security-updates-fixing-five-critical-vulnerabilities/