Security Advisory 2023-021

Critical Vulnerabilities in SAP Products

April 17, 2023 — v1.0

TLP:CLEAR

History:

- *17/04/2023 — v1.0 – Initial publication*

Summary

On April 11, 2023, SAP released 24 patches for various products, which contain five critical severity fixes that impact SAP Diagnostics Agent, SAP Business Client, SAP NetWeaver Process Integration, SAP BusinessObjects Business Intelligence Platform, and SAP NetWeaver Application Server for ABAP Platform [1]:

- Multiple vulnerabilities in SAP Diagnostics Agent - **CVE-2023-27497** and **CVE-2023-27267** (CVSS score 10.0);
- Update to Security Note released on April 2018 Patch Day: Security updates for the browser control Google Chromium delivered with SAP Business Client - (CVSS score 10.0);
- Improper access control in SAP NetWeaver AS Java - **CVE-2022-41272** (CVSS score 9.9);
- Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform - **CVE-2023-28765** (CVSS score 9.8);
- Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform - **CVE-2023-27269** (CVSS score 9.6).

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-2023-27497**: Due to missing authentication and input sanitisation of code, the EventLogServiceCollector of SAP Diagnostics Agent - version 720, allows an attacker to execute malicious scripts on all connected Diagnostics Agents running on Windows. On successful exploitation, the attacker can completely compromise confidentiality, integrity, and availability of the system [2];
- **CVE-2023-27267**: Due to missing authentication and insufficient input validation, the OSCommand Bridge of SAP Diagnostics Agent - version 720, allows an attacker with deep knowledge of the system to execute scripts on all connected Diagnostics Agents. On successful exploitation, the attacker can completely compromise confidentiality, integrity, and availability of the system [3];
- **CVE-2022-41272**: An unauthenticated attacker over the network can attach to an open interface exposed through JNDI by the User Defined Search (UDS) of SAP NetWeaver

Process Integration (PI) - version 7.50 and make use of an open naming and directory API to access services that can be used to perform unauthorised operations affecting users and data across the entire system. This allows the attacker to have full read access to user data, make limited modifications to user data, and degrade the performance of the system, leading to a high impact on confidentiality and a limited impact on the availability and integrity of the application [4];

- **CVE-2023-28765**: An attacker with basic privileges in SAP Business Objects Business Intelligence Platform (Promotion Management) - versions 420, 430, can access the lcmbiar file and further decrypt it. After this, the attacker can gain access to BI user's passwords and depending on the privileges of the BI user, the attacker can perform operations that can completely compromise the application [5];
- **CVE-2023-27269**: An attacker with non-administrative authorisations can exploit a directory traversal flaw in an available service to overwrite system files. In this attack, no data can be read, but potentially critical OS files can be overwritten making the system unavailable [6].

Affected products

- **CVE-2023-27497** and **CVE-2023-27267**: SAP Diagnostics Agent (OSCommand Bridge and EventLogServiceCollector) version **720** [1];
- Security updates for the Google Chromium browser control delivered with SAP Business Client: SAP Business Client versions **6.5, 7.0, 7.70** [1];
- **CVE-2022-41272**: SAP NetWeaver Process Integration version **7.50** [1];
- **CVE-2023-28765**: SAP BusinessObjects Business Intelligence Platform (Promotion Management) versions **420, 430** [1];
- **CVE-2023-27269**: SAP NetWeaver Application Server for ABAP and ABAP Platform versions **700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791** [1].

Recommendations

CERT-EU firmly recommends applying the security fixes for these critical vulnerabilities. It is also recommended to apply the other 19 patches.

References

[1] https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html

[2] https://www.cve.org/CVERecord?id=CVE-2023-27497

[3] https://www.cve.org/CVERecord?id=CVE-2023-27267

[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41272

[5] https://www.cve.org/CVERecord?id=CVE-2023-28765

[6] https://www.cve.org/CVERecord?id=CVE-2023-27269