National Cyber Security Centre

2304140128-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

SAP Diagnostics Agent, SAP BusinessObjects Business Intelligence Platform and SAP NetWeaver Vulnerabilities.

Friday 14th April, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

SAP have released security updates to address two critical vulnerabilities affecting SAP Diagnostics Agent, SAP BusinessObjects Business Intelligence Platform and one high severity vulnerability affecting SAP Netweaver.

The three vulnerabilities are:

- CVE-2023-29186 - CVSS 8.7

  Directory traversal flaw impacting SAP NetWeaver (BI CONT ADD ON)

- CVE-2023-27267 - CVSS 9.0

  Insufficient input validation and missing authentication issue impacting the OSCommand Bridge of SAP Diagnostics Agent (OSCommand Bridge and EventLogServiceCollector)

- CVE-2023-28765 - CVSS 9.8

  Information disclosure vulnerability impacting SAP BusinessObjects Business Intelligence Platform (Promotion Management)

The security updates also included five updates to previously addressed critical vulnerabilities.

Products Affected

The following SAP products are affected by these vulnerabilities:

- CVE-2023-29186

  - SAP NetWeaver (BI CONT ADDON)

  - Versions - 707, 737, 747, 757

- CVE-2023-27267

  - SAP Diagnostics Agent (OSCommand Bridge and EventLogServiceCollector)

  - Version – 720

- CVE-2023-28765

  - SAP BusinessObjects Business Intelligence Platform (Promotion Management)

  - Versions – 420, 430

SAP's updates to previously addressed critical vulnerabilities should be reviewed for the following products.

- CVE-2022-41272
  - SAP NetWeaver Process Integration
  - Version – 7.50
- 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

Impact

Exploitation of CVE-2023-29186 could allow an attacker to exploit a directory traversal flaw in a report to upload and overwrite files on the SAP server.

Exploitation of CVE-2023-27267 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.

Exploitation of CVE-2023-28765 allows an attacker with basic privileges to gain access to the lcmbiar file and decrypt it. This would enable the attacker to access users passwords contained on the platform and and allow them to perform additional malicious actions from the compromised accounts.

To date, there have been no reports of the active exploitation of these vulnerabilities.

Recommendations

The NCSC recommends organisations apply the relevant SAP security updates including the updates to previously addressed critical vulnerabilities as soon as possible.

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie