Critical SAP Security Notes

March Patch Day 2023

Bibin Mathew, SAP

March 16, 2023

Public

Very High Priority Security Notes (March 2023)

Very High Priority (CVSS > 8.9) Security Notes Released

1. 3245526 - [CVE-2023-25616] Code Injection vulnerability in SAP Business Objects Business Intelligence Platform (CMC)
2. 3283438 - [CVE-2023-25617] OS Command Execution vulnerability in SAP Business Objects Business Intelligence Platform (Adaptive Job Server)
3. 3252433 - [CVE-2023-23857] Improper Access Control in SAP NetWeaver AS for Java
4. 3294595 - [CVE-2023-27269] Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform
5. 3302162 - [CVE-2023-27500] Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform

We strongly advise our customers to apply these security notes immediately to protect against potential exploits and to ensure secure configuration of their SAP landscape.

3245526 - [CVE-2023-25616] Code Injection vulnerability in SAP Business Objects Business Intelligence Platform (CMC)

- **Released on:** March 2023 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP Business Objects Business Intelligence Platform (CMC)
- **Impact:** Complete compromise of confidentiality, integrity and availability
- **Vulnerabilities:**
    1. Code Injection vulnerability – Very High
       CVSS Score: 9.9; CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- **Workaround:** Refer to the Solution section

3283438 - [CVE-2023-25617] OS Command Execution vulnerability in SAP Business Objects Business Intelligence Platform (Adaptive Job Server)

- **Released on:** March 2023 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP Business Objects Business Intelligence Platform (Adaptive Job Server)
- **Impact:** Complete compromise of confidentiality, integrity and availability
- **Vulnerabilities:**
    1. OS Command Execution vulnerability – Very High
       CVSS Score: 9.0; CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
- **Workaround:** Refer to the Solution section

3252433 - [CVE-2023-23857] Improper Access Control in SAP NetWeaver AS for Java

- **Released on:** March 2023 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP NetWeaver AS for Java
- **Impact:** Complete compromise of availability, limited compromise on confidentiality and integrity
- **Vulnerabilities:**

  1. Improper Access Control – Very High
     CVSS Score: 9.9; CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H

- **FAQ:** 3299806

3294595 - [CVE-2023-27269] Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform

- **Released on:** March 2023 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP NetWeaver AS for ABAP and ABAP Platform
- **Impact:** Complete compromise of integrity and availability
- **Vulnerabilities:**
  1. Directory Traversal vulnerability – Very High
     CVSS Score: 9.6; CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H
- **Workaround:** Refer to the Solution section

3302162 - [CVE-2023-27500] Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform

- **Released on:** March 2023 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP NetWeaver AS for ABAP and ABAP Platform
- **Impact:** Complete compromise of integrity and availability
- **Vulnerabilities:**
    1. Directory Traversal vulnerability – Very High
    CVSS Score: 9.6; CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H
- **Workaround:** Refer to the Solution section

Thank you.

Contact information:

Bibin Mathew
bibin.mathew@sap.com