



# Critical SAP Security Notes

## January Patch Day 2023

Bibin Mathew, SAP  
January 19, 2023

Public

# Very High Priority Security Notes (January 2023)

## Very High Priority (CVSS > 8.9) Security Notes Released

1. 3275391 - [CVE-2023-0016] SQL Injection vulnerability in SAP Business Planning and Consolidation MS
2. 3262810 - [CVE-2023-0022] Code Injection vulnerability in SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP)
3. 3268093 - [CVE-2023-0017] Improper access control in SAP NetWeaver AS for Java
4. 3089413 - [CVE-2023-0014] Capture-replay 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.**

# 3275391 - [CVE-2023-0016] SQL Injection vulnerability in SAP Business Planning and Consolidation MS

- **Released on:** January 2023 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP Business Planning and Consolidation MS(Microsoft Platform)
- **Impact:** Complete compromise of confidentiality, integrity and availability
- **Vulnerabilities:**
  1. SQL Injection vulnerability – Very High  
CVSS Score: 9.9; CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- **FAQ:** [3279017](#)

# 3262810 - [CVE-2023-0022] Code Injection vulnerability in SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP)

- **Released on:** January 2023 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP)
- **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:L/UI:N/S:C/C:H/I:L/A:H
- **Workaround:** Refer to solution section

# 3268093 - [CVE-2023-0017] Improper access control in SAP NetWeaver AS for Java

- **Released on:** January 2023 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP NetWeaver AS for Java
- **Impact:** Complete compromise of confidentiality and integrity. Limited compromise of availability
- **Vulnerabilities:**
  1. Improper access control – Very High  
CVSS Score: 9.4; CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

# 3089413 - [CVE-2023-0014] Capture-replay vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform

- **Released on:** January 2023 Patch Day
- **Priority:** **Very High**
- **Product Affected:** SAP NetWeaver AS for ABAP and ABAP Platform
- **Impact:** Complete compromise of confidentiality, integrity and availability
- **Vulnerabilities:**
  1. Capture-replay vulnerability – Very High  
CVSS Score: 9.0; CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
- **FAQ:** [3281854](#)

# Thank you.

Contact information:

Bibin Mathew  
bibin.mathew@sap.com