مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

SAP Security Updates - February 2026

Tracking #:432318381

Date:11-02-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SAP released its monthly Security Patch Day updates, delivering 26 new Security Notes and 1 updated note addressing vulnerabilities across a wide range of SAP products.

TECHNICAL DETAILS:

SAP released its February 2026 Security Patch Day, addressing 26 new security vulnerabilities and 1 update to a previously released security note.

Key Statistics:

- Critical Severity: 2 vulnerabilities (CVSS 9.6 - 9.9)
- High Severity: 8 vulnerabilities (CVSS 7.3 - 8.8)
- Affected Products: SAP NetWeaver, SAP S/4HANA, SAP CRM, SAP BusinessObjects BI Platform, SAP Commerce Cloud, and SAP Supply Chain Management.

CRITICAL VULNERABILITIES

1. Code Injection in SAP CRM and SAP S/4HANA (Scripting Editor)
CVE: CVE-2026-0488
CVSS Score: 9.9 (Critical)
Priority: Critical
Affected Products:

- SAP CRM and SAP S/4HANA (Scripting Editor)
- Versions: S4FND 102-109, SAP_ABA 700, WEBCUIF 700, 701, 730, 731, 746-748, 800, 801

Vulnerability Description:
A code injection vulnerability exists in the Scripting Editor component of SAP CRM and SAP S/4HANA. This flaw allows attackers to inject and execute arbitrary code within the application context, potentially leading to complete system compromise.

2. Missing Authorization Check in SAP NetWeaver Application Server ABAP
CVE: CVE-2026-0509
CVSS Score: 9.6 (Critical)
Priority: Critical
Affected Products:

- SAP NetWeaver Application Server ABAP and ABAP Platform
- Versions: KRNL64NUC 7.22, 7.22EXT; KRNL64UC 7.22, 7.22EXT, 7.53; KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, 9.18, 9.19

Vulnerability Description:
A critical authorization bypass vulnerability allows attackers to circumvent access controls and perform unauthorized actions without proper authentication checks. This affects core ABAP platform functionality.

HIGH SEVERITY VULNERABILITIES
3. XML Signature Wrapping in SAP NetWeaver AS ABAP
Note: 3697567 | **CVE:** CVE-2026-23687 | **CVSS:** 8.8
Versions: SAP_BASIS 700-758, 804, 916-918

Impact: Authentication bypass, man-in-the-middle attacks, unauthorized access

4. Denial of Service in SAP Supply Chain Management
Note: 3703092 | **CVE:** CVE-2026-23689 | **CVSS:** 7.7
Versions: SCMAPO 713, 714; SCM 700-702, 712
Impact: System unavailability, supply chain disruption, financial losses

5. Missing Authorization Check in SAP Solution Tools Plug-In
Note: 3705882 | **CVE:** CVE-2026-24322 | **CVSS:** 7.7
Versions: ST-PI 2008_1_700, 2008_1_710, 740, 758
Impact: Unauthorized system configuration access, privilege escalation

6. Denial of Service in SAP BusinessObjects BI Platform
Note: 3654236 | **CVE:** CVE-2026-0490 | **CVSS:** 7.5
Note: 3678282 | **CVE:** CVE-2026-0485 | **CVSS:** 7.5
Versions: ENTERPRISE 430, 2025, 2027
Impact: BI platform unavailability, disruption of reporting and analytics

7. Race Condition in SAP Commerce Cloud
Note: 3692405 | **CVE:** CVE-2025-12383 | **CVSS:** 7.4
Versions: HY_COM 2205, COM_CLOUD 2211, 2211-JDK21
Impact: Transaction manipulation, data corruption, customer data exposure

8. Open Redirect in SAP BusinessObjects BI Platform
Note: 3674246 | **CVE:** CVE-2026-0508 | **CVSS:** 7.3
Versions: ENTERPRISE 430, 2025, 2027
Impact: Phishing attacks, credential harvesting, malware distribution

RECOMMENDATIONS:

- SAP strongly recommends immediate patching, prioritizing Critical and High severity notes to reduce the risk of compromise in production landscape.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/february-2026.html