AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Përditësime Sigurie SAP – Shkurt 2026

Data: 11/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

SAP ka publikuar përditësimet mujore të **Security Patch Day**, që përfshijnë:

- **26 Security *Notes* të reja**
- **1 *Security Note* të përditësuar**

që adresojnë dobësi në një gamë të gjerë produktesh SAP.

Statistika Kryesore

- **Kritike:** 2 dobësi (CVSS 9.6 – 9.9)
- **Të Larta:** 8 dobësi (CVSS 7.3 – 8.8)
- **Produkte të prekura:**
  - SAP NetWeaver
  - SAP S/4HANA
  - SAP CRM
  - SAP BusinessObjects BI Platform
  - SAP Commerce Cloud
  - SAP Supply Chain Management

Informacione Teknike

DOBËSITË KRITIKE

1. Code Injection në SAP CRM dhe SAP S/4HANA (Scripting Editor)

- **CVE:** CVE-2026-0488
- **CVSS:** 9.9 (Kritike)
- **Prioriteti:** Kritik

Produkte të prekura:

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

Përshkrim:
Ekziston një dobësi e tipit *code injection* në komponentin Scripting Editor, që lejon injektim dhe ekzekutim kodi arbitrar brenda kontekstit të aplikacionit, duke çuar potencialisht në kompromet të plotë të sistemit.

2. Missing Authorization Check në SAP NetWeaver Application Server ABAP

- **CVE:** CVE-2026-0509
- **CVSS:** 9.6 (Kritike)
- **Prioriteti:** Kritik

Produkte të prekura:

- SAP NetWeaver Application Server ABAP dhe ABAP Platform
- Versionet:
  - 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

Përshkrim:
Dobësi kritike e anashkalimit të autorizimit që lejon sulmuesit të shmangin kontrollet e aksesit dhe të kryejnë veprime të paautorizuara pa verifikime të duhura autentikimi. Prek funksionalitetin bazë të platformës ABAP.

DOBËSITË ME RREZIKSHMËRI TË LARTË

3. XML Signature Wrapping në SAP NetWeaver AS ABAP

- **Note:** 3697567
- **CVE:** CVE-2026-23687
- **CVSS:** 8.8
- **Versione:** SAP_BASIS 700–758, 804, 916–918

Ndikimi:
Anashkalim autentikimi, sulme man-in-the-middle, akses i paautorizuar.

4. Denial of Service në SAP Supply Chain Management

- **Note:** 3703092
- **CVE:** CVE-2026-23689
- **CVSS:** 7.7
- **Versione:** SCMAPO 713, 714; SCM 700–702, 712

Ndikimi:
Mosdisponueshmëri sistemi, ndërprerje zinxhiri furnizimi, humbje financiare.

5. *Missing Authorization Check në SAP Solution Tools Plug-In*

- **Note:** 3705882
- **CVE:** CVE-2026-24322
- **CVSS:** 7.7
- **Versione:** ST-PI 2008_1_700, 2008_1_710, 740, 758

Ndikimi:
Akses i paautorizuar në konfigurime sistemi, rritje privilegjesh.

6. Denial of Service në SAP BusinessObjects BI Platform

- **Note:** 3654236 | CVE-2026-0490 | CVSS 7.5
- **Note:** 3678282 | CVE-2026-0485 | CVSS 7.5
- **Versione:** ENTERPRISE 430, 2025, 2027

Ndikimi:
Mosdisponueshmëri e platformës BI, ndërprerje e raportimit dhe analitikës.

7. Race Condition në SAP Commerce Cloud

- **Note:** 3692405
- **CVE:** CVE-2025-12383
- **CVSS:** 7.4
- **Versione:** HY_COM 2205; COM_CLOUD 2211; 2211-JDK21

Ndikimi:
Manipulim transaksionesh, korruptim të dhënash, ekspozim i të dhënave të klientëve.

8. Open Redirect në SAP BusinessObjects BI Platform

- **Note:** 3674246
- **CVE:** CVE-2026-0508
- **CVSS:** 7.3
- **Versione:** ENTERPRISE 430, 2025, 2027

Ndikimi:
Sulme phishing, vjedhje kredencialesh, shpërndarje malware.

Rekomandime

Rekomandohet fuqimisht **aplikimi i menjëhershëm i patch-eve**, duke i dhënë prioritet dobësive me rrezikshmëri **Kritike dhe të Lartë**, për të reduktuar rrezikun e kompromet imit në mjediset e prodhimit.

Referenca

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