AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

SAP Security Patch Day Advisory – Prill 2026

Data: 14/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

SAP ka publikuar përditësimet mujore që adresojnë një numër të konsiderueshëm dobësish në platformat kryesore enterprise duke adresuar:

- **19 dobësi të reja**
- **1 shënim sigurie të përditësuar**

Këto prekin platforma si:

- SAP S/4HANA
- SAP ERP
- SAP NetWeaver
- SAP BusinessObjects

Dobësia më kritike (**CVSS 9.9**) është një **SQL Injection**, e cila mund të çojë në kompromet të plotë të databazës.

Informacione Teknike

Detaje të Dobësisë:

Dobësia Kritike (Veprim i Menjëhershëm)

CVE-2026-27681 – SQL Injection (CVSS: 9.9 – Kritike)
Produkte të prekura:

- SAP Business Planning and Consolidation (BPC)
- SAP Business Warehouse (BW)

Versionet:

- HANABPC 810, BPC4HANA 300
- SAP_BW 750, 752, 753, 754, 755, 756, 757, 758, 816

Dobësi me Rrezikshmëri të Lartë

CVE-2026-34256 – Mungesë kontrolli autorizimi (CVSS: 7.1)
Produkte të prekura:

- SAP ERP
- SAP S/4HANA (Private Cloud dhe On-Premise)

Versionet:

- SAP_FIN 618, 720, 730
- EA-FIN 617, 700
- SAPSCORE 135
- S4CORE 102–109
- EA-APPL 600, 602, 603, 604, 605, 606

Dobësi me Rrezikshmëri Mesatare

- CVE-2025-64775 – SAP BusinessObjects BI Platform (CVSS: 6.5)
- CVE-2026-34264 – SAP HCM për S/4HANA (CVSS: 6.5)
- CVE-2026-34261 – SAP Business Analytics & SAP Content Management (CVSS: 6.5)
- CVE-2026-27677 – SAP S/4HANA OData Service (CVSS: 6.5)
- CVE-2026-27678 – SAP S/4HANA Backend OData Service (CVSS: 6.5)
- CVE-2026-27679 – SAP S/4HANA Frontend OData Service (CVSS: 6.5)
- CVE-2026-0512 – SAP Supplier Relationship Management (CVSS: 6.1)
- CVE-2026-27674 – SAP NetWeaver AS Java (CVSS: 6.1)
- CVE-2026-34257 – SAP NetWeaver AS ABAP (CVSS: 6.1)
- CVE-2026-34262 – SAP HANA Cockpit & DB Explorer (CVSS: 5.0)
- CVE-2026-27673 – SAP S/4HANA (CVSS: 4.9)
- CVE-2026-27672 – Material Master Application (CVSS: 4.3)
- CVE-2026-27676 – SAP S/4HANA OData Service (CVSS: 4.3)

Rekomandime

Subjektet që përdorin mjedise SAP duhet ta trajtojnë këtë përditësim si **prioritet të lartë**, me ndërhyrje të menjëhershme për dobësinë kritike, për të parandaluar:

- shfrytëzim të dobësive
- rrjedhje të të dhënave
- ndërprerje operacionale

Referenca

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