مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# SAP Security Patch Day Advisory – April 2026

Tracking #:432318784

Date:14-04-2026



**TLP: WHITE**

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SAP released its monthly Security Patch Day updates, addressing 19 new vulnerabilities and 1 updated security note across multiple core enterprise platforms including SAP S/4HANA, SAP ERP, SAP NetWeaver, and SAP BusinessObjects.

## TECHNICAL DETAILS:

On 14 April 2026, SAP released its monthly Security Patch Day updates, addressing 19 new vulnerabilities and 1 updated security note across multiple core enterprise platforms including SAP S/4HANA, SAP ERP, SAP NetWeaver, and SAP BusinessObjects. The most critical issue (CVSS 9.9) involves a SQL Injection vulnerability affecting SAP Business Planning and Consolidation (BPC) and SAP Business Warehouse (BW), which could lead to full database compromise.

**Critical Vulnerability (Immediate Action Required)**

- **CVE-2026-27681 – SQL Injection** (CVSS Score: 9.9-Critical)
- **Affected Products:**
  - SAP Business Planning and Consolidation (BPC)
  - SAP Business Warehouse (BW)
- **Versions:**
  - HANABPC 810, BPC4HANA 300
  - SAP_BW 750, 752, 753, 754, 755, 756, 757, 758, 816

**High Severity Vulnerability:**

- **CVE-2026-34256 – Missing Authorization Check (**CVSS Score: 7.1 – High**)**
- **Affected Products:**
  - SAP ERP
  - SAP S/4HANA (Private Cloud and On-Premise)
- **Versions:**
  - SAP_FIN 618, 720, 730
  - EA-FIN 617, 700
  - SAPSCORE 135
  - S4CORE 102–109
  - EA-APPL 600, 602, 603, 604, 605, 606

**Medium Severity Vulnerabilities:**

- CVE-2025-64775 – SAP BusinessObjects BI Platform (CVSS: 6.5)
- CVE-2026-34264 – SAP HCM for 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)

- CVE-2025-42899 – SAP S4CORE (Updated) (CVSS: 4.3)
- CVE-2026-24318 – SAP BusinessObjects BI Platform (CVSS: 4.2)
- CVE-2026-27683 – SAP BusinessObjects BI Platform (CVSS: 4.1)

**Low Severity Vulnerabilities:**

- CVE-2026-27680 – SAP NetWeaver AS ABAP (CVSS: 3.1)
- CVE-2026-27675 – SAP Landscape Transformation (CVSS: 2.0)

## RECOMMENDATIONS:

- Organizations running SAP environments treat this update as high priority, with immediate remediation required for critical vulnerability to prevent exploitation, data breaches, and operational disruption.

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/april-2026.html