مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

SAP January 2026 Security Updates

Tracking #:432318249

Date:14-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SAP has released its January 2026 security patch package containing 17 security notes addressing critical vulnerabilities across enterprise SAP environments.

TECHNICAL DETAILS:

SAP has released its January 2026 security patch package containing 17 security notes addressing critical vulnerabilities across enterprise SAP environments. This release includes four HotNews vulnerabilities with CVSS ratings up to 9.9, four High priority issues, seven Medium priority fixes, and two Low priority updates. The patches affect SAP S/4HANA, SAP HANA database, SAP NetWeaver, SAP Wily Introscope, and various application components.

Technical Details – Vulnerability Breakdown

1. Critical Severity Vulnerabilities (CVSS 9.0 – 10.0)

- **CVE-2026-0501 – SQL Injection**
  - **Product**: SAP S/4HANA (Financials – General Ledger)
  - **Affected Versions**: S4CORE 102–109
  - **CVSS**: 9.9 (Critical)
- **CVE-2026-0500 – Remote Code Execution**
  - **Product**: SAP Wily Introscope Enterprise Manager (WorkStation)
  - **Affected Versions**: WILY_INTRO_ENTERPRISE 10.8
  - **CVSS**: 9.6 (Critical)
- **CVE-2026-0498 – Code Injection**
  - **Product**: SAP S/4HANA (Private Cloud & On-Premise)
  - **Affected Versions**: S4CORE 102–109
  - **CVSS**: 9.1 (Critical)
- **CVE-2026-0491 – Code Injection**
  - **Product**: SAP Landscape Transformation
  - **Affected Versions**: DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2018_1_752, 2020
  - **CVSS**: 9.1 (Critical)

2. High Severity Vulnerabilities (CVSS 8.0 – 8.9)

- **CVE-2026-0492 – Privilege Escalation**
  - **Product**: SAP HANA Database
  - **Affected Versions**: HDB 2.00
  - **CVSS**: 8.8
- **CVE-2026-0507 – OS Command Injection**
  - **Product**: SAP Application Server for ABAP / NetWeaver RFCSDK
  - **Affected Versions**: Kernel 7.53–9.16, NWRFCSDK 7.50, KRNL64UC 7.53
  - **CVSS**: 8.4
- **CVE-2026-0511 / 0496 / 0495 – Multiple Vulnerabilities**
  - **Product**: SAP Fiori App (Intercompany Balance Reconciliation)
  - **CVSS**: 8.1
  - Version(s) - UIAPFI70 500, 600, 700, 800, 900, 901, 902, S4CORE 102, 103, 104, 105,

106, 107, 108

- **CVE-2026-0506 – Missing Authorization Check**
  - **Product**: SAP NetWeaver AS ABAP / ABAP Platform
  - **Affected Versions**: SAP_BASIS 700–816
  - **CVSS**: 8.1
  - Version(s) - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816

RECOMMENDATIONS:

- Prioritize patching of all Critical and High-severity SAP Notes.
- Apply Medium-severity patches during scheduled maintenance windows.
- Review role-based access controls (RBAC) for affected SAP modules.

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/january-2026.html