مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

SAP Security Patch Day (November 2025)

Tracking #:432317990

Date:12-11-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SAP released its monthly Security Patch Day updates, addressing 18 new security notes and providing two updates to existing ones, focusing on vulnerabilities that could enable remote code execution and various injection attacks across its product ecosystem.

TECHNICAL DETAILS:

SAP has released its November 2025 Security Patch Day updates, addressing 20 security notes, including 18 new and 2 updated vulnerabilities across multiple SAP products such as SAP NetWeaver, SAP HANA, SAP Solution Manager, SAP Business Connector, and SAP GUI for Windows.

The release contains three critical vulnerabilities rated with CVSS scores up to 10.0, which could allow remote code execution, insecure key management, and data manipulation without user interaction.

Organizations leveraging SAP environments are strongly advised to apply the patches immediately, prioritizing critical vulnerabilities that enable remote compromise, especially those affecting SQL Anywhere Monitor, NetWeaver AS Java, and Solution Manager.

CVE ID	Title / Description	Affected Product	CVSS Score
CVE-2025-42890	Insecure Key & Secret Management vulnerability	SQL Anywhere Monitor (Non-GUI) – SYBASE_SQL_ANYWHERE_SERVER 17.0	10.0 (Critical)
CVE-2025-42944	Security Hardening for Insecure Deserialization	SAP NetWeaver AS Java – SERVERCORE 7.50	10.0 (Critical)
CVE-2025-42887	Code Injection vulnerability	SAP Solution Manager – ST 720	9.9 (Critical)
CVE-2025-42940	Memory Corruption vulnerability	SAP CommonCryptoLib – CRYPTOLIB 8	7.5 (High)
CVE-2025-42895	Code Injection vulnerability	SAP HANA JDBC Client – HDB_CLIENT 2.0	6.9 (Medium)
CVE-2025-42892	OS Command Injection vulnerability	SAP Business Connector – SAP BC 4.8	6.8 (Medium)
CVE-2025-42894	Path Traversal vulnerability	SAP Business Connector – SAP BC 4.8	6.8 (Medium)
CVE-2025-42884	JNDI Injection vulnerability	SAP NetWeaver Enterprise Portal – EP-BASIS 7.50, EP-RUNTIME 7.50	6.5 (Medium)
CVE-2025-42924	Open Redirect vulnerability	SAP S/4HANA (SAP E-Recruiting BSP) – S4ERECRT 100, 200, ERECRUIT 600–802	6.1 (Medium)
CVE-2025-42893	Open Redirect vulnerability	SAP Business Connector – SAP BC 4.8	6.1 (Medium)
CVE-2025-42886	Reflected Cross-Site Scripting (XSS)	SAP Business Connector – SAP BC 4.8	6.1 (Medium)

	vulnerability		
CVE-2025-42885	Missing Authentication vulnerability	SAP HANA 2.0 (hdbrss) – HDB 2.00	5.8 (Medium)
CVE-2025-42888	Information Disclosure vulnerability	SAP GUI for Windows – BC-FES-GUI 8.00, 8.10	5.5 (Medium)
CVE-2025-42889	SQL Injection vulnerability	SAP Starter Solution (PL SAFT) – SAP_APPL 600–616, SAP_FIN 617–720, S4CORE 100–104	5.4 (Medium)
CVE-2025-42919	Information Disclosure vulnerability	SAP NetWeaver AS Java – ENGINEAPI 7.50, EP-BASIS 7.50	5.3 (Medium)
CVE-2025-42897	Information Disclosure vulnerability	SAP Business One (SLD) – B1_ON_HANA 10.0, SAP-M-BO 10.0	5.3 (Medium)
CVE-2025-42899	Missing Authorization Check	SAP S4CORE (Manage Journal Entries) – S4CORE 104–108	4.3 (Medium)
CVE-2025-42882	Missing Authorization Check	SAP NetWeaver AS for ABAP – SAP_BASIS 700–758, 816	4.3 (Medium)
CVE-2025-23191	Cache Poisoning through Header Manipulation vulnerability	SAP Fiori for SAP ERP – SAP_GWFND 740–758	3.1 (Low)
CVE-2025-42883	Insecure File Operations vulnerability	SAP NetWeaver AS for ABAP (Migration Workbench) – SAP_BASIS 700–758, 816	2.7 (Low)

RECOMMENDATIONS:

Organizations leveraging SAP environments are strongly advised to apply the patches immediately, prioritizing critical vulnerabilities.

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/november-2025.html