مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-SAP Products

Tracking #:432317362

Date:11-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SAP released security patches addressing 14 newly discovered vulnerabilities across its product portfolio, including one critical and several high-severity flaws that pose immediate risks to enterprise environments.

TECHNICAL DETAILS:

SAP released security patches addressing 14 newly discovered vulnerabilities across its product portfolio, including one critical and several high-severity flaws that pose immediate risks to enterprise environments. The most severe vulnerability (CVE-2025-42989, CVSS 9.6) affects SAP NetWeaver Application Server for ABAP, enabling privilege escalation and risking the integrity and availability of core business systems.

Additional high-severity issues impact SAP GRC, SAP Business Warehouse, and SAP BusinessObjects BI, threatening data confidentiality, system availability, and operational continuity. Organizations using these SAP components must prioritize immediate patching to mitigate the risk of exploitation and potential business disruption

Key Vulnerabilities:

CVE ID	Affected Component	Description & Impact	CVSS Score	Urgency
CVE-2025-42989	SAP NetWeaver AS for ABAP	Missing authorization check in RFC inbound processing, enabling privilege escalation and broad system access for authenticated users. Exploitation can critically impact integrity and availability. Affects kernel versions 7.89, 7.93, 9.14, 9.15.	9.6	Critical
CVE-2025-42982	SAP GRC AC Plugin	Information disclosure flaw allows non-admin users to initiate sensitive transactions and manipulate credentials, risking confidentiality, integrity, and availability. Affects Versions – GRCPINW V1100_700, V1100_731	8.8	High
CVE-2025-42983	SAP Business Warehouse, Plug-In Basis	Missing authorization check enables authenticated users to delete arbitrary database tables, risking data loss and system inoperability. Impacts PI_BASIS and SAP_BW. Affects Versions – PI_BASIS 2006_1_700, 701, 702, 731, 740, SAP_BW 750, 751, 752, 753, 754, 755, 756, 757, 758, 914, 915	8.5	High
CVE-2025-23192	SAP BusinessObjects BI Workspace	XSS vulnerability allows unauthenticated attackers to inject malicious scripts in shared workspaces, risking data theft and UI manipulation. Affects Versions – ENTERPRISE 430, 2025, 2027	8.2	High

Other Vulnerabilities:

High Severity

- CVE-2025-42977: SAP NetWeaver Visual Composer
- CVE-2025-42989: SAP NetWeaver Application Server for ABAP
- CVE-2025-42994, CVE-2025-42995, CVE-2025-42996: SAP MDM Server
- CVE-2025-42982: SAP GRC AC Plugin
- CVE-2025-42983: SAP Business Warehouse, SAP Plug-In Basis
- CVE-2025-23192: SAP BusinessObjects BI Workspace

Medium Severity

- CVE-2025-42993: SAP S/4HANA (Enterprise Event Enablement)
- CVE-2025-31325: SAP NetWeaver (ABAP Keyword Documentation)
- CVE-2025-42984: SAP S/4HANA (Manage Central Purchase Contract application)
- CVE-2025-42998: SAP Business One Integration Framework
- CVE-2025-42987: SAP S/4HANA (Manage Processing Rules - For Bank Statement)
- CVE-2025-42991: SAP S/4HANA (Bank Account Application)

Low Severity

- CVE-2025-42988: SAP Business Objects Business Intelligence Platform
- CVE-2025-42990: SAPUI5 applications

RECOMMENDATIONS:

Organizations using affected SAP components are strongly advised to apply security patches immediately.

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/june-2025.html