مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - SAP

Tracking #:432317471

Date:09-07-2025

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

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that SAP has released a security bulletin addressing multiple vulnerabilities, with severities ranging from critical to low.

TECHNICAL DETAILS:

SAP released its monthly Security Patch Day updates, addressing 27 vulnerabilities across its enterprise product suite. Among them, seven were rated critical, with the most severe being CVE-2025-30012, a composite vulnerability in SAP Supplier Relationship Management (SRM) Live Auction Cockpit, carrying a CVSS score of 10.0 (Critical).

This critical flaw aggregates multiple underlying vulnerabilities — CVE-2025-30009, CVE-2025-30010, CVE-2025-30011, and CVE-2025-30018 — which, if exploited, may allow unauthenticated attackers to execute arbitrary code, escalate privileges, and gain complete control over the affected SAP system.

Organizations running SAP SRM or other enterprise modules should prioritize patching as exploitation risks are elevated due to the complexity and severity of these vulnerabilities.

Vulnerability Details (Including but not limited to):

- **CVE-2025-30012 -** Multiple vulnerabilities in SAP Supplier Relationship Management (Live Auction Cockpit)
  - **Priority**: Critical
  - **CVSS**: 10.0
  - **Product –** SAP Supplier Relationship Management (Live Auction Cockpit)
  - **Version –** SRM_SERVER 7.14
- **CVE-2025-42967 -** Code Injection vulnerability in SAP S/4HANA and SAP SCM (Characteristic Propagation)
  - **Priority**: Critical
  - **CVSS**: 9.9
  - **Product –** SAP S/4HANA and SAP SCM (Characteristic Propagation)
  - **Versions –** SCMAPO 713, 714, S4CORE 102, 103, 104, S4COREOP 105, 106, 107, 108, SCM 700, 701, 702, 712
- **CVE-2025-42980** - Insecure Deserialization in SAP NetWeaver Enterprise Portal Federated Portal Network
  - **Priority**: Critical
  - **CVSS**: 9.1
  - **Product –** SAP NetWeaver Enterprise Portal Federated Portal Network
  - **Version –** EP-RUNTIME 7.50
- **CVE-2025-42964** - Insecure Deserialization in SAP NetWeaver Enterprise Portal Administration
  - **Priority**: Critical
  - **CVSS**: 9.1

- **Product** – SAP NetWeaver Enterprise Portal Administration
- **Version** – EP-RUNTIME 7.50

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the necessary patches released by SAP at the earliest.

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/july-2025.html