مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - SAP

Tracking #:432317813

Date:14-10-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that SAP has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

SAP has released its October 2025 Security Updates to address multiple vulnerabilities identified across various SAP products. Successful exploitation of these vulnerabilities could allow remote code execution, directory traversal, unrestricted file uploads, denial-of-service conditions, unauthorized system access, information disclosure, security misconfiguration exploitation, cross-site request forgery, memory corruption, and exposure of sensitive data.

Critical Vulnerabilities

- **[CVE-2025-42944] Security Hardening for Insecure Deserialization**
  Product: SAP NetWeaver AS Java, Version: SERVERCORE 7.50
  CVSS: 10.0
- **Update to September 2025 Note: [CVE-2025-42944] Insecure Deserialization (RMI-P4)**
  Product: SAP NetWeaver AS Java, Version: SERVERCORE 7.50
  CVSS: 10.0
- **[CVE-2025-42937] Directory Traversal**
  Product: SAP Print Service, Versions: SAPSPRINT 8.00, 8.10
  CVSS: 9.8
- **[CVE-2025-42910] Unrestricted File Upload**
  Product: SAP Supplier Relationship Management, Versions: SRMNXP01 100, 150
  CVSS: 9.0

High-Severity Vulnerabilities

- **[CVE-2025-5115] Denial of Service (DoS)**
  Product: SAP Commerce Cloud, Versions: HY_COM 2205, COM_CLOUD 2211, 2211-JDK21
  CVSS: 7.5
- **[CVE-2025-48913] Security Misconfiguration**
  Product: SAP Data Hub Integration Suite, Version: CX_DATAHUB_INT_PACK 2205
  CVSS: 7.1

Medium-Severity Vulnerabilities

- **Update to January 2025 Note: [CVE-2025-0059] Information Disclosure**
  Product: SAP NetWeaver Application Server ABAP, Versions: KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.12, 9.14
  CVSS: 6.0
- **[CVE-2025-42901] Code Injection (BAPI Browser)**
  Product: SAP Application Server for ABAP, Versions: SAP_BASIS 700–758, 816
  CVSS: 5.4
- **[CVE-2025-42908] Cross-Site Request Forgery (CSRF)**
  Product: SAP NetWeaver Application Server for ABAP, Versions: KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.16
  CVSS: 5.4
- **[CVE-2025-42906] Directory Traversal**

Product: SAP Commerce Cloud, Version: COM_CLOUD 2211
CVSS: 5.3

- **[CVE-2025-42902] Memory Corruption**
  Product: SAP NetWeaver AS ABAP & ABAP Platform, Versions: KRNL64NUC 7.22–7.22EXT, KRNL64UC 7.22–7.93, KERNEL 7.22–9.16
  CVSS: 5.3
- **[CVE-2025-42939] Missing Authorization Check**
  Product: SAP S/4HANA, Versions: S4CORE 104–109
  CVSS: 4.3
- **Update to April 2025 Note: [CVE-2025-31331] Authorization Bypass**
  Product: SAP NetWeaver, Versions: SAP_ABA 700–75I
  CVSS: 4.3
- **[CVE-2025-42903] User Enumeration & Sensitive Data Exposure via RFC**
  Product: SAP Financial Service Claims Management, Versions: INSURANCE 803–806, S4CEXT 107–109
  CVSS: 4.3

Low-Severity Vulnerabilities

- **[CVE-2025-31672] Deserialization Vulnerability**
  Product: SAP BusinessObjects, Versions: ENTERPRISE 430, 2025, 2027
  CVSS: 3.5
- **[CVE-2025-42909] Security Misconfiguration**
  Product: SAP Cloud Appliance Library Appliances, Version: TITANIUM_WEBAPP 4.0
  CVSS: 3.0

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by SAP.

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/october-2025.html