مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - SAP

Tracking #:432319097

Date:09-06-2026

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 June 2026 Security Updates, addressing multiple vulnerabilities affecting SAP NetWeaver, SAP Commerce Cloud, SAP S/4HANA, SAP Business Objects, SAP Fiori, and other SAP products. Several of the vulnerabilities are rated Critical and could allow authentication bypass, remote code execution, memory corruption, directory traversal, unauthorized access to sensitive systems and data, and other security impacts.

Vulnerability Details

Critical Vulnerabilities

- **CVE-2026-44748** – XML Signature Wrapping in SAML Authentication in SAP NetWeaver AS ABAP and ABAP Platform
- **CVE-2026-27671** – Memory Corruption Vulnerability in Application Server ABAP of SAP NetWeaver and ABAP Platform
- **CVE-2026-22732** – Potential Spring Security Vulnerability in SAP Commerce Cloud and SAP Data Hub
- **CVE-2026-40128** – Directory Traversal Vulnerability in SAP NetWeaver Application Server Java (Web Container)

High Severity Vulnerabilities

- **CVE-2026-29145** – Multiple Vulnerabilities in Apache Tomcat within SAP Commerce Cloud
- **CVE-2026-44751** – Missing Authorization Check in Application Server ABAP of SAP NetWeaver and ABAP Platform

Medium Severity Vulnerabilities

- **CVE-2026-44754** – Missing Caller Identification Check in ODP Data Replication APIs
- **CVE-2026-44744** – SQL Injection Vulnerability in SAP S/4HANA
- **CVE-2026-44746** – Reflected Cross-Site Scripting (XSS) Vulnerability in SAP NetWeaver AS Java (JDBC Test Servlet)
- **CVE-2026-44757** – Cross-Site Scripting (XSS) Vulnerability in SAP Wily Introscope Enterprise Manager
- **CVE-2026-44750** – Missing Authorization Check in SAP MDG (Review Match Groups Application)
- **CVE-2026-44755** – Email Spoofing Vulnerability in SAP Business Objects Business Intelligence Platform
- **CVE-2026-24315** – Path Traversal Vulnerability in SAP Fiori (Launchpad)

Low Severity Vulnerabilities

- **CVE-2026-44743** – Security Misconfiguration Vulnerability in SAP Business Objects
- **CVE-2025-68161** – Potential Vulnerability in Apache Log4j Library Used by SAP NetWeaver AS Java

Successful exploitation of these vulnerabilities could allow attackers to bypass authentication and authorization controls, execute arbitrary code, gain unauthorized access to sensitive information, escalate privileges, manipulate database queries, access restricted files and resources, and compromise the confidentiality, integrity, and availability of affected SAP systems.

Note
Refer to the official SAP security advisory for detailed information regarding affected products, impacted software versions, fixed releases, and recommended mitigation measures.

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/june-2026.html