مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - SAP

Tracking #:432316959

Date:11-03-2025

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

SAP has released its monthly Security Patch Day updates, addressing a total of 21 new Security Notes and 3 updates to previously released notes. These updates address a range of vulnerabilities, including Cross-Site Scripting (XSS), Missing Authorization checks, Broken Authentication, and Information Disclosure, across various SAP products.

High-Severity Vulnerabilities:

- **CVE-2025-27434**: Cross-Site Scripting (XSS) in SAP Commerce (Swagger UI) with a CVSS score of 8.8.
- **CVE-2025-26661**: Missing Authorization Check in SAP NetWeaver (ABAP Class Builder) with a CVSS score of 8.8.
- **CVE-2024-38286**: Multiple vulnerabilities in Apache Tomcat within SAP Commerce Cloud with a CVSS score of 8.6.

Updates to Previously Released Notes:

- **CVE-2025-24876**: Authentication bypass in SAP Approuter (updated from February 2025) with a CVSS score of 8.1.
- **CVE-2024-39592**: Missing Authorization Check in SAP PDCE (updated from July 2024) with a CVSS score of 7.7.

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/march-2025.html