مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - SAP

Tracking #:432316862

Date:12-02-2025

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 released its February 2025 Security Patches on February 11, 2025, addressing 21 new and updated SAP Security Notes, including six High Priority vulnerabilities. The patch addresses vulnerabilities in multiple SAP applications, with the most critical issues affecting SAP NetWeaver AS Java, SAP Business Objects, SAP Supplier Relationship Management, and SAP Approuter.

High-Severity Vulnerabilities:

1. **SAP NetWeaver AS Java**: A Cross-Site Scripting vulnerability (CVE-2024-22126) with a CVSS score of 8.8.
2. **SAP BusinessObjects**: An Improper Authorization Check vulnerability (CVE-2025-0064) in the Central Management Console, with a CVSS score of 8.7.
3. **SAP Supplier Relationship Management**: A Path traversal vulnerability (CVE-2025-25243) in the Master Data Management Catalog, with a CVSS score of 8.6.
4. **SAP Approuter**: An Authentication bypass vulnerability (CVE-2025-24876) affecting versions 16.7.1 and earlier, with a CVSS score of 8.1.
5. **SAP Enterprise Project Connection**: Multiple vulnerabilities (CVE-2024-38819, CVE-2024-38820, CVE-2024-38828) with a CVSS score of 7.5.
6. **SAP HANA extended application services**: An Open Redirect Vulnerability (CVE-2025-24868) in the User Account and Authentication service, with a CVSS score of 7.1.

Successful exploitation of these vulnerabilities could lead to various security risks, including unauthorized access, data breaches, and system disruption.

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/february-2025.html