مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - SAP

Tracking #:432318944

Date:12-05-2026

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 May 2026 security updates, addressing multiple vulnerabilities across SAP products, including two critical flaws affecting SAP S/4HANA and SAP Commerce Cloud. These updates mitigate risks such as SQL injection, missing authentication, OS command injection, code injection, and cross-site scripting.

Vulnerability Details

Critical

- **CVE-2026-34260 (CVSS 9.6)**
  SQL Injection Vulnerability in SAP S/4HANA (SAP Enterprise Search for ABAP)
- **CVE-2026-34263 (CVSS 9.6)**
  Missing Authentication Check in SAP Commerce Cloud Configuration

High

- **CVE-2026-34259 (CVSS 8.2)**
  OS Command Injection Vulnerability in SAP Forecasting & Replenishment

Medium

- **CVE-2026-40135 (CVSS 6.5)**
  OS Command Injection Vulnerability in SAP NetWeaver Application Server for ABAP and ABAP Platform
- **CVE-2026-40133 (CVSS 6.3)**
  Missing Authorization Check in SAP S/4HANA Condition Maintenance
- **CVE-2026-40137 (CVSS 6.1)**
  Cross-Site Scripting (XSS) Vulnerability in Business Server Pages Application (TAF_APPLAUNCHER)
- **CVE-2026-0502 (CVSS 5.4)**
  Cross-Site Request Forgery (CSRF) in SAP BusinessObjects Business Intelligence Platform
- **CVE-2026-40132 (CVSS 5.4)**
  Missing Authorization Check in SAP Strategic Enterprise Management
- **CVE-2025-68161 (CVSS 4.8)**
  Potential Improper Certificate Validation in SAP Commerce Cloud (Apache Log4j)
- **CVE-2026-34258 (CVSS 4.7)**
  Content Spoofing Vulnerability in SAPUI5 (Search UI)
- **CVE-2026-27682 (CVSS 4.7)**
  Reflected Cross-Site Scripting (XSS) Vulnerability in SAP NetWeaver Application Server ABAP
- **CVE-2026-40136 (CVSS 4.3)**
  Denial of Service (DoS) in SAP Financial Consolidation
- **CVE-2026-40134 (CVSS 4.3)**
  Missing Authorization Check in SAP Incentive and Commission Management
- **CVE-2026-40129 (CVSS 4.3)**
  Code Injection Vulnerability in SAP Application Server ABAP for SAP NetWeaver and ABAP Platform

Low

- **CVE-2026-40131 (CVSS 3.4)**
  SQL Injection Vulnerability in SAP HANA Deployment Infrastructure (HDI) Deploy Library

Impact

Successful exploitation of these vulnerabilities could allow attackers to execute arbitrary commands, inject malicious code, bypass authentication, exploit authorization flaws, access sensitive data, or disrupt services. This may lead to unauthorized access, privilege escalation, system compromise, configuration manipulation, or broader impact across affected SAP environments.

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/may-2026.html