مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

SAP Security Updates - March 2026

Tracking #:432318556

Date:10-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SAP released 15 new security notes as part of its monthly SAP Security Patch Day addressing vulnerabilities across several enterprise products.

TECHNICAL DETAILS:

SAP released 15 new security notes as part of its monthly SAP Security Patch Day addressing vulnerabilities across several enterprise products. The vulnerabilities affect critical SAP platforms including NetWeaver, Supply Chain Management, Business One, Business Warehouse, and SAP GUI. The most severe issues include code injection and insecure deserialization vulnerabilities with CVSS scores up to 9.8, which could allow attackers to execute malicious code or compromise SAP environments.

Patch Overview
Total Security Notes Released: 15

- Critical: 2
- High: 1
- Medium: 11
- Low: 1

CRITICAL VULNERABILITIES
1. Code Injection in SAP Quotation Management Insurance

- Security Note: 3698553
- CVE: CVE-2019-17571
- CVSS Score: 9.8 (Critical)
- Affected Product: SAP Quotation Management Insurance (FS-QUO 800)

2. Insecure Deserialization in SAP NetWeaver Enterprise Portal

- Security Note: 3714585
- CVE: CVE-2026-27685
- CVSS Score: 9.1 (Critical)
- Affected Product: SAP NetWeaver Enterprise Portal Administration (EP-RUNTIME 7.50)

High Severity Vulnerability
Denial of Service in SAP Supply Chain Management

- Security Note: 3719502
- CVE: CVE-2026-27689
- CVSS Score: 7.7
- Affected Product: SAP Supply Chain Management

Affected Versions

- SCMAPO 713, 714
- S4CORE 102–104
- S4COREOP 105–109
- SCM 700–712

RECOMMENDATIONS:

- SAP strongly recommends immediate patching, prioritizing Critical and High severity notes to reduce the risk of compromise in production landscape.

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-2026.html