مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

SAP July 2026 Security Updates

Tracking #:432319293

Date:14-07-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SAP has released its July 2026 Security Patch Day updates, addressing 16 new Security Notes, one GitHub Security Advisory, and three updates to previously released Security Notes.

TECHNICAL DETAILS:

SAP has released its July 2026 Security Patch Day updates, addressing 16 new Security Notes, one GitHub Security Advisory, and three updates to previously released Security Notes. The release remediates multiple vulnerabilities affecting core SAP products, including SAP NetWeaver Application Server ABAP, SAP Approuter, SAP Commerce Cloud, SAP Integration Suite, SAProuter, SAP S/4HANA, SAP NetWeaver Java, SAP Fiori, and SAP HANA.

The most severe vulnerability, CVE-2026-44747 (CVSS 9.9), is a memory corruption vulnerability in SAP NetWeaver Application Server ABAP that could allow a low-privileged attacker to compromise the confidentiality, integrity, and availability of affected systems.

Other critical vulnerabilities include an HTTP Request Smuggling flaw in SAP Approuter (CVE-2026-27690), insecure sample credentials in SAP Commerce Cloud (CVE-2026-44761), and an updated advisory for a Directory Traversal vulnerability in SAP NetWeaver AS Java (CVE-2026-40128).

Noted Vulnerability Details:

- CVE-2026-44747
  - Severity: Critical
  - CVSS: 9.9
  - Component: SAP NetWeaver Application Server ABAP
  - Vulnerability: Memory Corruption
- CVE-2026-27690
  - Severity: Critical
  - CVSS: 9.1
  - Component: SAP Approuter
  - Vulnerability: HTTP Request Smuggling
- CVE-2026-44761
  - Severity: Critical
  - CVSS: 9.1
  - Component: SAP Commerce Cloud
  - Vulnerability: Insecure Sample Credentials
- CVE-2026-40128
  - Severity: Critical (Updated June 2026 Security Note)
  - CVSS: 9.0
  - Component: SAP NetWeaver Application Server Java (Web Container)
  - Vulnerability: Directory Traversal
- CVE-2026-40860
  - Severity: High
  - CVSS: 8.8
  - Component: SAP Integration Suite (Edge Integration Cell)
  - Vulnerability: Multiple Apache Camel Vulnerabilities

    - Includes fixes for third-party vulnerabilities:
        - CVE-2026-40453
        - CVE-2026-33454
- CVE-2026-0487
    - Severity: High
    - CVSS: 8.4
    - Component: SAProuter (Windows)
    - Vulnerability: DLL Hijacking
- CVE-2026-44752
    - Severity: High
    - CVSS: 8.2
    - Component: SAP NetWeaver AS Java Configuration Wizard
    - Vulnerability: Cross-Site Scripting (XSS)
- CVE-2026-44745
    - Severity: High
    - CVSS: 8.1
    - Component: SAP Approuter
    - Vulnerability: Open Redirect
- Multiple Apache Tomcat CVEs
    - Severity: High
    - CVSS: 8.1
    - Component: SAP Commerce Cloud
    - Affected CVEs:
        - CVE-2026-43512
        - CVE-2026-41293
        - CVE-2026-43515
    - Addresses vulnerabilities in bundled Apache Tomcat components.
- CVE-2026-58233
    - Severity: High
    - CVSS: 7.6
    - Component: SAP Change and Transport System Attach Tool (ctsattach)
    - Vulnerability: Remote Code Execution

RECOMMENDATIONS:

Immediate Actions:

- Apply all relevant SAP July 2026 Security Notes according to SAP's priority guidance.
- Prioritize remediation of all Critical vulnerabilities, especially CVE-2026-44747, CVE-2026-27690, CVE-2026-44761, and CVE-2026-40128.

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/july-2026.html