مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache Tomcat

Tracking #:432318776

Date:13-04-2026

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

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Apache Tomcat. These flaws could lead to sensitive data exposure, authentication bypass, credential compromise, and security control evasion.

TECHNICAL DETAILS:

Key Vulnerabilities
High Severity

- **CVE-2026-29146 – Padding Oracle Attack in EncryptInterceptor**
  The EncryptInterceptor component is vulnerable to a padding oracle attack, allowing attackers to decrypt sensitive data without access to the encryption key.
- **CVE-2026-34486 – EncryptInterceptor Bypass (Regression Flaw)**
  An error in the fix for CVE-2026-29146 allows bypassing the EncryptInterceptor, resulting in exposure of sensitive data in unencrypted form.

Medium Severity

- **CVE-2026-34500 – OCSP Soft-Fail Authentication Bypass**
  CLIENT_CERT authentication may incorrectly succeed when OCSP validation errors occur, even when soft-fail behavior is disabled.

Fixed Versions

- Apache Tomcat 11.0.21 or later
- Apache Tomcat 10.1.54 or later
- Apache Tomcat 9.0.117 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Apache Tomcat.

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://lists.apache.org/thread/lzt04z2pb3dc5tk85obn80xygw3z1p0w
- https://lists.apache.org/thread/9510k5p5zdvt9pkkgtyp85mvwxo2qrly
- https://lists.apache.org/thread/7rcl4zdxryc8hy3htyfyxkbqpxjtfdl2