مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache Tomcat

Tracking #:432318445

Date:23-02-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Apache Tomcat and Apache Tomcat Native that may affect system security and allow security protections to be bypassed.

TECHNICAL DETAILS:

Multiple vulnerabilities have been identified in Apache Tomcat and Apache Tomcat Native that could allow security constraint bypass, client certificate authentication bypass, and OCSP revocation check bypass.

Vulnerability Details

CVE-2026-24733 – Security Constraint Bypass via HTTP/0.9

- **Severity:** Low
- Apache Tomcat did not properly restrict HTTP/0.9 requests to supported methods. Under certain configurations, this could allow bypass of security constraints that rely on HTTP method validation.

CVE-2025-66614 – Client Certificate Verification Bypass via Virtual Host Mapping

- **Severity:** Moderate
- Apache Tomcat did not validate consistency between the TLS SNI hostname and the HTTP Host header. In multi-virtual-host environments, this could allow bypass of client certificate authentication in specific configurations.

CVE-2026-24734 – OCSP Revocation Check Bypass

- **Severity:** Moderate
- When using OCSP responders, Apache Tomcat Native did not fully verify OCSP response freshness and validation, which could allow revocation checks to be bypassed under certain conditions.

Affected Products

- Apache Tomcat 11.0.0-M1 to 11.0.14
- Apache Tomcat 10.1.0-M1 to 10.1.49
- Apache Tomcat 9.0.0.M1 to 9.0.112
- Apache Tomcat 11.0.0-M1 to 11.0.17
- Apache Tomcat 10.1.0-M7 to 10.1.51
- Apache Tomcat 9.0.83 to 9.0.114
- Apache Tomcat Native 2.0.0 to 2.0.11
- Apache Tomcat Native 1.3.0 to 1.3.4
- Earlier End-of-Life (EOL) versions may also be affected

Fixed Versions

- Apache Tomcat 11.0.15 or later
- Apache Tomcat 10.1.50 or later
- Apache Tomcat 9.0.113 or later
- Apache Tomcat 11.0.18 or later
- Apache Tomcat 10.1.52 or later
- Apache Tomcat 9.0.115 or later

- Apache Tomcat Native 2.0.12 or later
- Apache Tomcat Native 1.3.5 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released 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/6xk3t65qpn1myp618krtfotbjn1qt90f
- https://lists.apache.org/thread/vw6lxtlh2qbqwpb61wd3sv1flm2nttw7
- https://lists.apache.org/thread/292dlmx3fz1888v6v16221kpozq56gml