مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

# Critical RCE Vulnerability in Apache Tomcat

Tracking #:432316978

Date:17-03-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability, CVE-2025-24813, has been discovered in Apache Tomcat, allowing attackers to fully compromise vulnerable servers with a single PUT API request.

## TECHNICAL DETAILS:

A critical remote code execution (RCE) vulnerability, CVE-2025-24813, has been discovered in Apache Tomcat, allowing attackers to fully compromise vulnerable servers with a single PUT API request. The vulnerability is actively exploited in the wild and affects multiple versions of Tomcat, leveraging the default session persistence mechanism and partial PUT request handling. Attackers can upload a malicious Java session file via PUT, followed by a GET request to trigger deserialization and execute arbitrary code. Immediate mitigation is necessary, as this attack requires no authentication and is difficult to detect with traditional security solutions.

**Vulnerability Details**

- Vulnerability ID: CVE-2025-24813

Affected Software:

- Apache Tomcat 11.0.0-M1 to 11.0.2
- Apache Tomcat 10.1.0-M1 to 10.1.34
- Apache Tomcat 9.0.0.M1 to 9.0.98

Mitigation:

- Apache Tomcat 11.0.3 and later
- Apache Tomcat 10.1.35 and later
- Apache Tomcat 9.0.99 and later

**Exploit Mechanism:**

1. **Malicious Session Upload:** The attacker sends a PUT request containing a serialized Java session file with embedded malicious payload, which gets stored in Tomcat's session directory.
2. **Execution via GET Request:** The attacker sends a GET request with a JSESSIONID pointing to the malicious session, triggering deserialization and executing arbitrary Java code.

**Exploitation Conditions:**

- The application has servlet write enabled (default is disabled).
- Tomcat uses file session persistence with the default storage location.
- The application contains a deserialization exploitation library.

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade Tomcat to patched versions.

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/j5fkjv2k477os90nczf2v9l61fb0kkgq