مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Apache Tomcat

Tracking #:432317143

Date:29-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that The Apache Software Foundation has released security updates addressing two significant vulnerabilities affecting Apache Tomcat servers.

TECHNICAL DETAILS:

The Apache Software Foundation has released urgent security updates to address two significant vulnerabilities in Apache Tomcat, a widely deployed open-source Java Servlet container. These vulnerabilities-CVE-2025-31650 and CVE-2025 can result in denial of service (DoS) and security rule bypass, respectively, if left unpatched.

Vulnerability Details:

1. **CVE-2025-31650: Denial of Service (DoS) via Invalid HTTP Prioritization Header**
   - Severity: High
   - Impact: Memory leak leads to OutOfMemoryException, potentially causing server crashes and downtime.
   - Affected Versions:
     - Tomcat 11.0.0-M2 to 11.0.5
     - Tomcat 10.1.10 to 10.1.39
     - Tomcat 9.0.76 to 9.0.102
   - Root Cause: Improper cleanup of failed HTTP requests with invalid priority headers.

2. **CVE-2025-31651: Rewrite Rule Bypass**
   - Severity: Low
   - Impact: Potential bypass of rewrite security rules, risking unauthorized access.
   - Affected Versions:
     - Tomcat 11.0.0-M1 to 11.0.5
     - Tomcat 10.1.0-M1 to 10.1.39
     - Tomcat 9.0.0.M1 to 9.0.102
   - Root Cause: Incomplete validation in specific, uncommon rewrite rule configurations.

Fixed Versions:

- Apache Tomcat 11.0.6 or later
- Apache Tomcat 10.1.40 or later
- Apache Tomcat 9.0.104 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions of Apache Tomcat to the fixed or latest versions at the earliest.

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/y14yjrf40w2236hwjv7gmhs65csn42gj
- https://lists.apache.org/thread/sxzchc0mkp7kd238dzothwqh2cww6l7b