مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Multiple Vulnerabilities in Apache Tomcat
Tracking #:432317867
Date:28-10-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apache has released security updates to address multiple vulnerabilities in Apache Tomcat. The flaws could allow remote code execution, log manipulation, or denial-of-service conditions under certain configurations.

TECHNICAL DETAILS:

Vulnerability Details
CVE-2025-55752 — URL Rewrite Regression (Remote Code Execution)
- **Severity:** High
- A flaw in URL rewrite handling may allow attackers to bypass security constraints and potentially execute arbitrary code via malicious HTTP PUT requests.

CVE-2025-55754 — ANSI Escape Sequence Injection in Logs
- **Severity:** Critical
- Improper escaping of ANSI sequences in log messages could allow attackers to inject commands or manipulate console behavior on Windows systems.

CVE-2025-61795 — Denial-of-Service via Multipart File Uploads
- **Severity:** Low
- Temporary files from multipart uploads may not be deleted immediately after errors, potentially causing disk space exhaustion and denial-of-service.

Successful exploitation of these vulnerabilities could allow attackers to execute arbitrary code, manipulate administrative consoles, gain unauthorized access, or cause denial-of-service conditions on affected systems.

Fixed Versions
- Apache Tomcat 9.0.110, 10.1.47, and 11.0.12 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache.

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/38vqp0v1fg4gr8c6lvm15wj6k67hxzxd
- https://lists.apache.org/thread/kslp83vxhtzw9lfj0753otwx9yl36y7l
- https://lists.apache.org/thread/njwfh0pon9kw6xorl1zl40dxcnnq1hnf