مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache Tomcat

Tracking #:432317387

Date:17-06-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Apache Tomcat that could be exploited to cause denial-of-service (DoS) conditions, privilege bypass, and installer abuse on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-48976 – DoS via Multipart Header Overload**
  Severity: High
  A malicious request containing a large number of multipart headers could consume excessive memory, resulting in a denial of service.
- **CVE-2025-48988 – Multipart Upload Abuse Enables DoS**
  Severity: High
  Attackers could flood servers with requests containing a high number of multipart parts, exhausting memory resources and causing a denial of service.
- **CVE-2025-49124 – Windows Installer Side-Loading Risk**
  Severity: Low
  On Windows systems, the Tomcat installer used icacls.exe without specifying a full path, potentially allowing a side-loading attack if a malicious executable with the same name was present in the system's path.
- **CVE-2025-49125 – Security Constraint Bypass in Pre/PostResources**
  Severity: Medium
  When web applications use PreResources or PostResources mounted outside the root, Tomcat could allow unintended access via alternate paths, potentially bypassing security constraints.

Fixed Versions:

- Apache Tomcat 11.0.8 or later
- Apache Tomcat 10.1.42 or later
- Apache Tomcat 9.0.106 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/w7dbnfyqn1yc05kbqqbbyct7wbomv7lf
- https://lists.apache.org/thread/z2d63tflwvqvdg3crz8d1sy2v3xsr4n8
- https://lists.apache.org/thread/khdh7y3y1wogjocrz8jy8mmqzmgc9y5o
- https://lists.apache.org/thread/0jwb3d3sjyfk5m6xnnj7h9m7ngxz23db