مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Denial-of-Service Vulnerability in Apache Tomcat

Tracking #:432316322
Date:24-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in Apache Tomcat, a widely used Java servlet container. This vulnerability could be exploited to potentially cause a denial-of-service (DoS) attack on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-38286**
- **Severity:** Important
- A vulnerability exists in Apache Tomcat's TLS handshake process that could allow attackers to trigger an OutOfMemoryError, effectively crashing the server.
- A successful exploitation of this vulnerability can result in:
  - **Service disruption:** Critical applications and services running on Tomcat may become unavailable.
  - **Resource exhaustion:** The server may become unresponsive due to depleted memory resources.
  - **Operational downtime:** Organizations may face significant downtime, affecting business operations and user accessibility.

Affected Versions:

- Apache Tomcat 11.0.0-M1 to 11.0.0-M20
- Apache Tomcat 10.1.0-M1 to 10.1.24
- Apache Tomcat 9.0.13 to 9.0.89

Fixed Versions:

- For Apache Tomcat 11: Upgrade to 11.0.0-M21 or later.
- For Apache Tomcat 10.1: Upgrade to 10.1.25 or later.
- For Apache Tomcat 9.0: Upgrade to 9.0.90 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed 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/8xm50bvr6rhbjkdtbxl5x4d20dpfy83p