مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical RCE Vulnerability in Apache Tomcat

Tracking #:432316657

Date:23-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Apache Tomcat that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-56337**
- Vulnerability Type: Time-of-check Time-of-use (TOCTOU) Race Condition
- The vulnerability stems from an incomplete mitigation of a previous vulnerability (**CVE-2024-50379**). The flaw is exploitable on case-insensitive file systems where Tomcat's default servlet has write functionality enabled. By manipulating specific paths, attackers can bypass security measures and upload malicious JSP files, leading to remote code execution.
- Exploitation of this vulnerability can allow attackers to execute arbitrary code on the affected server, potentially granting them complete control over the system.

Affected Versions:

- Apache Tomcat 11.0.0-M1 to 11.0.1
- Apache Tomcat 10.1.0-M1 to 10.1.33
- Apache Tomcat 9.0.0.M1 to 9.0.97

Fixed Versions:

- **Apache Tomcat 11.0.2** or later
- **Apache Tomcat 10.1.34** or later
- **Apache Tomcat 9.0.98** or later

Java Configuration Requirements

Depending on the Java version used with Apache Tomcat, additional configuration may be necessary:

- **Java 8 or Java 11:** Explicitly set the system property sun.io.useCanonCaches to false.
- **Java 17:** Ensure the system property sun.io.useCanonCaches, if set, is set to false.
- **Java 21 and later:** No further action is required.

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://nvd.nist.gov/vuln/detail/CVE-2024-56337