مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Apache Tomcat

Tracking #:432316642

Date:18-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Apache Tomcat has released a critical security update to address a vulnerability in Apache Tomcat that can lead to Remote Code Execution (RCE).

TECHNICAL DETAILS:

Apache Tomcat has released a critical security update to address a vulnerability in Apache Tomcat that can lead to Remote Code Execution (RCE).

Vulnerability Details:

- **CVE-2024-50379: Remote Code Execution (RCE)**
- CVSS score of 9.8 Critical
- The issue arises when the default servlet is write-enabled (i.e., the readonly initialization parameter is set to false), and the system is running on a case-insensitive file system.
- Under these conditions, an attacker can exploit the vulnerability by concurrently reading and uploading the same file under high load. This process bypasses Tomcat's case sensitivity checks, causing an uploaded file to be incorrectly processed as a JSP (JavaServer Pages) file. The result is the potential execution of arbitrary code on the server, leading to remote code execution.

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

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/y6lj6q1xnp822g6ro70tn19sgtjmr80r