Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 358 31-12-2024

Name: Apache Tomcat Vulnerability CVE-2024-56337 Exposes Servers to RCE Attacks

Threat Classification: Remote Code Execution (RCE) Vulnerability

Affected Software / Services:

- 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

Summary:

Apache Tomcat is vulnerable to a Remote Code Execution (RCE) attack due to a Time-of-Check Time-of-Use (TOCTOU) race condition. The flaw originates from an incomplete mitigation for **CVE-2024-50379**, which allowed attackers to exploit case-insensitive file systems and bypass checks under specific conditions.

By exploiting concurrent file uploads and reads, attackers can disguise malicious payloads as Java Server Pages (JSP) files, enabling them to execute arbitrary code remotely. The vulnerability primarily affects servers with case-insensitive file systems where the default servlet has write access enabled **(readonly=false).**

The Apache Software Foundation has released updated versions to address the vulnerability, and additional configuration adjustments are recommended to fully mitigate the issue.

Severity	Critical
Attack Vector	Time-of-Check to Time-of-Use (TOCTOU) race condition.

Recommendations:

- Update to 11.0.2 or later, 10.1.34 or later, or 9.0.98 or later. Download latest version from the official Apache Tomcat page: https://tomcat.apache.org/
- For **Java 8 or 11**, explicitly set sun.io.useCanonCaches to false.
- For **Java 17**, verify that sun.io.useCanonCaches is set to false.
- For **Java 21 and later**, no action is needed.
- Set the servlet's readonly property to true to disable write access.
- Use a **case-sensitive file system** where possible to mitigate vulnerabilities relying on case-insensitivity.
- Restrict concurrent file read and upload operations where applicable.
- Implement robust logging and monitoring for suspicious file activities.
- Regularly audit server configurations to disable unnecessary services or components.
- Deploy strong access controls to secure upload directories and other sensitive server areas.