Remote Code Execution Bypass Addressed in Apache Tomcat Web Server

Overview

The Apache Software Foundation has addressed a vulnerability in Apache Tomcat. CVE-2024-56337 could allow attackers to execute remote code on affected systems. This flaw bypasses an incomplete mitigation for a previously identified remote code execution (RCE) vulnerability (CVE-2024-50379).

CVE-2024-56337 is a time-of-check time-of-use (TOCTOU) race condition vulnerability that impacts systems running Apache Tomcat with the default servlet write enabled (readonly set to false) on case-insensitive file systems.

Affected Products

- Apache Tomcat Versions:
    - 11.0.0-M1 to 11.0.1
    - 10.1.0-M1 to 10.1.33
    - 9.0.0-M1 to 9.0.97

Apache Tomcat is a widely used open-source web server and servlet container, needed for deploying Java-based web applications. Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch –** Upgrade to the latest versions: 11.0.2, 10.1.34, and 9.0.98. See Apache's advisory for patch guidance.
- Configure Java Properties Based on Version
    - For Java 8 or 11 - Explicitly set sun.io.useCanonCaches to false (default: true).
    - For Java 17 - Ensure sun.io.useCanonCaches, if set, is configured as false (default: false).
    - For Java 21 and later - No additional configuration is required, as the property and problematic cache have been removed.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190) – Exploitation of the TOCTOU race condition to gain initial access via Tomcat's default servlet.

Privilege Escalation

- Abuse Elevation Control Mechanism (T1548.002) – Exploitation of improperly configured Java properties to bypass security controls.

IoCs

There are no known IoCs associated with CVE-2024-56337 at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

This Apache Tomcat vulnerability (CVE-2024-56337) could impact a range of industries that rely on Java-based web applications, SaaS platforms, and hosting services. Key industries include:

- Technology and SaaS providers
- Healthcare
- Banking and Finance
- Telecommunications
- Government
- E-Commerce
- And others

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

NVD - CVE-2024-56337

[SECURITY] CVE-2024-56337 Apache Tomcat - RCE via write-enabled default servlet - CVE-2024-50379 mitigation was incomplete-Apache Mail Archives

Apache Tomcat® - Apache Tomcat 11 vulnerabilities