BREAKING CYBERSECURITY NEWS: APACHE TOMCAT VULNERABILITY ACTIVELY EXPLOITED JUST 30 HOURS AFTER PUBLIC DISCLOSURE

Vairav Cyber Security News Report

Date: March 18th, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A critical vulnerability in Apache Tomcat, identified as CVE-2025-24813, has been actively exploited in the wild just 30 hours after its public disclosure. This flaw enables remote code execution (RCE) or information disclosure under specific conditions, posing significant risks to affected systems. Organizations utilizing vulnerable versions of Apache Tomcat are advised to apply the necessary patches promptly to mitigate potential threats.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: CVE-2025-24813 is a vulnerability affecting Apache Tomcat versions 9.0.0-M1 to 9.0.98, 10.1.0-M1 to 10.1.34, and 11.0.0-M1 to 11.0.2. The flaw arises when the following conditions are met:

- Writes are enabled for the default servlet (disabled by default).
- Support for partial PUT is enabled (enabled by default).
- A target URL for security-sensitive uploads is a sub-directory of a target URL for public uploads.
- Attackers have knowledge of the names of security-sensitive files being uploaded.
- The security-sensitive files are also being uploaded via partial PUT.

The exploit, originally published by a Chinese forum user iSee857, is already available online.

Affected Entities/Industries: Organizations using the affected versions of Apache Tomcat across various industries are at risk, especially those that have not disabled the default servlet's write capabilities or are unaware of their server configurations regarding partial PUT support.

Potential Impact:

- **Financial Losses:** Exploitation could lead to unauthorized access, data breaches, or system compromises, resulting in financial damages.
- **Operational Downtime:** Successful attacks may disrupt services, leading to operational interruptions.

- **Data Exposure:** Sensitive information could be disclosed or altered without authorization.
- **Reputational Damage:** Organizations may suffer reputational harm due to security breaches.

Exploitation Methods: Attackers exploit this vulnerability by sending a PUT request containing a Base64-encoded serialized Java payload to Tomcat's session storage directory. This payload is then executed during deserialization when a GET request with the malicious session ID is sent. Notably, this exploit requires no authentication and is facilitated by Tomcat's support for partial PUT requests and file-based session storage.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Update Apache Tomcat to the latest patched versions: 9.0.99, 10.1.35, or 11.0.3.
- Disable write permissions for the default servlet if not explicitly required.
- Review and configure the server to handle partial PUT requests securely or disable them if unnecessary.

Security Best Practices

- Regularly audit server configurations and access controls.
- Implement robust input validation to prevent unauthorized file uploads.
- Maintain up-to-date backups and a tested incident response plan.

For Advanced Security Teams

- Monitor network traffic for unusual PUT and GET requests targeting Tomcat servers.
- Implement Web Application Firewalls (WAFs) to detect and block malicious payloads.
- Conduct regular security assessments and penetration testing to identify potential vulnerabilities.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/03/apache-tomcat-vulnerability-comes-under.html
- https://lab.wallarm.com/one-put-request-to-own-tomcat-cve-2025-24813-rce-is-in-the-wild/
- https://tomcat.apache.org/security-11.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com