Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apache Tomcat Hit by Active RCE Exploit Patch Before It's Too Late!

Date of Publication	Admiralty Code	TA Number
March 18, 2025	A1	TA2025082

Summary

First Seen: March 10, 2025
Affected Products: Apache Tomcat
Impact: A critical remote code execution (RCE) vulnerability, CVE-2025-24813, has been identified in Apache Tomcat, enabling attackers to take control of servers using a simple PUT request. Alarmingly, a public proof-of-concept (PoC) exploit was released just 30 hours after disclosure, leading to exploitation in the wild. To stay protected, update Apache Tomcat to the latest patched version immediately.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-24813	Apache Tomcat Remote Code Execution Vulnerability	Apache Tomcat	✗	✗	✓

Vulnerability Details

#1 A critical remote code execution (RCE) vulnerability, tracked as CVE-2025-24813, has been discovered in Apache Tomcat and is likely being exploited. This flaw allows attackers to gain control of vulnerable servers through a PUT API request, a method typically used to update existing resources.

#2 The vulnerability stems from how Apache Tomcat handles partial PUT requests when writing temporary files. Under specific conditions, attackers can exploit this weakness to access sensitive files or inject malicious content. In some cases, they can escalate the attack to achieve remote code execution (RCE). Successful exploitation requires several factors, including writable access to the default servlet, enabled partial PUT requests, and a predictable file path for sensitive uploads.

#3 If an application uses Tomcat's file-based session persistence and includes a vulnerable deserialization library, attackers can execute arbitrary code. The attack follows two simple steps: first, the attacker uploads a malicious Java session file via a PUT request, then triggers deserialization by referencing the compromised session ID in a GET request.

#4 A proof-of-concept (PoC) exploit was publicly released just 30 hours after disclosure, making widespread attacks more likely. Due to active exploitation, immediate patching is crucial. Apache strongly advises users to upgrade to Tomcat versions 11.0.3 or later, 10.1.35 or later, or 9.0.99 or later, which contain fixes for CVE-2025-24813.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-24813	Apache Tomcat Versions 11.0.0-M1 to 11.0.2, Apache Tomcat Versions 10.1.0-M1 to 10.1.34, Apache Tomcat Versions 9.0.0.M1 to 9.0.98	cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:*	CWE-502 CWE-44

Recommendations

Upgrade Immediately : Update Apache Tomcat to the latest patched versions (11.0.3 or later, 10.1.35 or later, or 9.0.99 or later) to safeguard against active exploits. Delaying the update could leave your servers vulnerable to remote code execution attacks.

Restrict PUT Requests: Disable the PUT method in Tomcat's configuration unless absolutely uploads and off partial PUT support if not required to minimize the attack surface.

Strengthen Access Controls: Disable write access for the default servlet to prevent unauthorized file uploads and enforce strong authentication to restrict access to administrative endpoints and sensitive directories.

Enhance Security Monitoring: Use intrusion detection systems (IDS) and log monitoring to spot unusual PUT or GET requests targeting session files. Also, review file storage locations to ensure sensitive files aren't accessible through public upload directories.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
T1588 Obtain Capabilities	**T1588.005** Exploits	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter
T1027 Obfuscated Files or Information	**T1068** Exploitation for Privilege Escalation		

Patch Details

To safeguard against the CVE-2025-24813 vulnerability, Upgrade Apache Tomcat to the latest patched versions (11.0.3 or later, 10.1.35 or later, or 9.0.99 or later)

Links: https://tomcat.apache.org/security-11.html , https://tomcat.apache.org/security-10.html , https://tomcat.apache.org/security-9.html

References

https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq

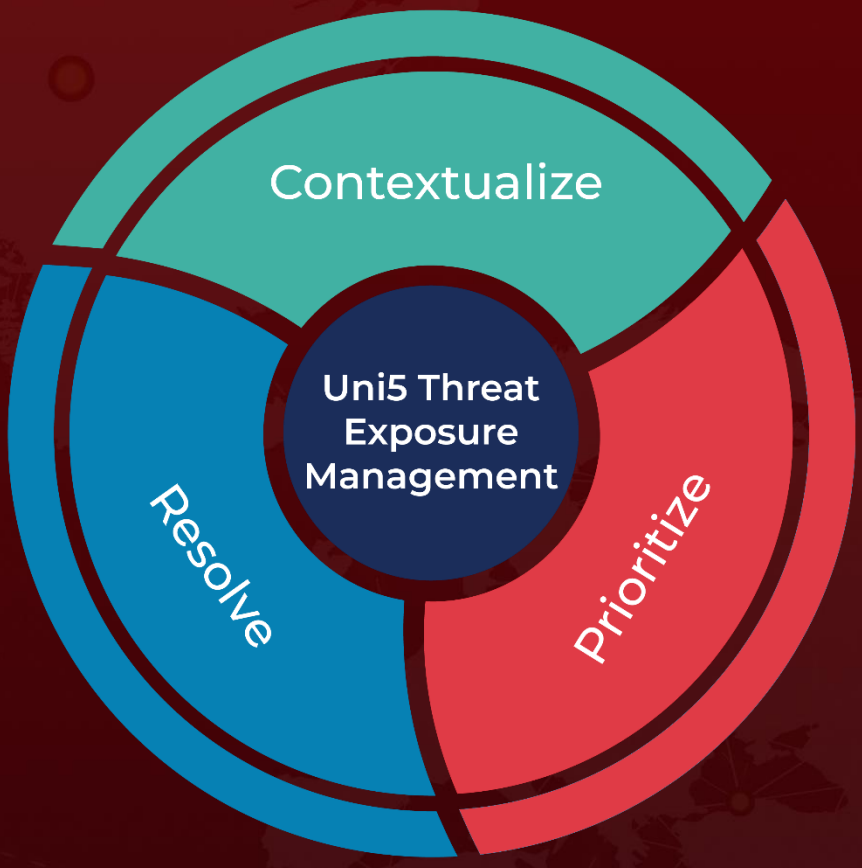
https://lab.wallarm.com/one-put-request-to-own-tomcat-cve-2025-24813-rce-is-in-the-wild/

https://github.com/absholi7ly/POC-CVE-2025-24813/blob/main/README.md

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 18, 2025 • 7:00 AM

More at www.hivepro.com