Apache Tomcat Vulnerability (CVE-2025-24813) Actively Exploited

Overview

A remote code execution (RCE) vulnerability in Apache Tomcat, CVE-2025-24813 (CVSS 9.8), is being actively exploited in the wild just 30 hours after public disclosure. The flaw allows attackers to upload and execute malicious files using a PUT request under specific conditions.

Attackers are leveraging Tomcat's session persistence mechanism and partial PUT request handling to execute arbitrary code. Exploitation begins with a PUT request that uploads a malicious serialized Java session file to Tomcat's session storage. Once the file is in place, the attacker triggers deserialization by sending a GET request with a specially crafted JSESSIONID, causing the malicious payload to execute.

For successful exploitation, several conditions must be met.

- Writes must be enabled for the default servlet, though this is disabled by default.
- Partial PUT requests must be supported, which is enabled by default in Tomcat.
- The application must be using Tomcat's file-based session persistence, and an exploitable library that allows deserialization attacks must be present.

If all these conditions are met, an attacker can achieve full system compromise.

Affected Products

- Apache Tomcat 9.x, 10.x, 11.x (specific versions listed above)
- Applications using file-based session storage in Tomcat
- Web applications allowing unauthenticated PUT requests

CVE-2025-24813 is being actively exploited and requires no authentication to execute. Attackers can view sensitive files or inject malicious content into existing files. Patching as soon as possible is highly recommended.

Aspire Protects

- **Patch –** Upgrade immediately to Apache Tomcat 9.0.99, 10.1.35, and 11.0.3. See Apache's advisory for details.
- Disable partial PUT support if not required.
- Restrict PUT and DELETE methods to trusted users only.
- Implement Web Application Firewall (WAF) rules to detect suspicious PUT requests.
- Monitor for unusual session files in Tomcat's storage directory.
- Enable logging and alerting for abnormal PUT/GET requests.

TTPs to Watch

Initial Access
- Exploit Public-Facing Application [T1190] – The attacker may exploit Apache Tomcat to gain access to a vulnerable system.

Execution
- Exploitation for Client Execution [T1203] – The attacker bypassed security measures using Tomcat's session deserialization.

Persistence
- Web Shell [T1505.003] – The attacker may upload and execute malicious JSP files to maintain long-term access.

Privilege Escalation
- Abuse Elevation Control Mechanism [T1548] – The attacker may leverage the RCE exploit to escalate privileges.

IoCs

- Suspicious PUT requests containing Base64-encoded payloads.
- Unauthorized modifications to session files in Tomcat's storage.
- GET requests with unusual JSESSIONID values attempting to trigger deserialization.

There are no other known IoCs associated with CVE-2025-24813 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 vulnerability could impact a wide range of industries. Industries/sectors include:

- Retail
- Finance
- Healthcare
- IT
- Government
- Manufacturing
- Energy
- Education
- 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-2025-24813

[SECURITY] CVE-2025-24813 Potential RCE and/or information disclosure and/or information corruption with partial PUT-Apache Mail Archives

One PUT Request to Own Tomcat: CVE-2025-24813 RCE is in the Wild - API Security