Security Advisory 2025-014

Critical Vulnerability in Apache Tomcat

2025-04-03 — v1.0

TLP:CLEAR

History:

- *03/04/2025 — v1.0 – Initial publication*

Summary

On March 10, 2025, Apache released a security advisory [1] regarding a critical vulnerability affecting the Apache Tomcat product.

It is recommended updating the affected assets to a fixed version of Apache Tomcat.

Technical Details

The vulnerability **CVE-2025-24813**, with a CVSS score of 9.8, lies in the Apache Tomcat's partial PUT feature. Under specific circumstances, successful exploitation allows attackers to execute code remotely on target systems via unsafe deserialisation [1,2].

An attacker could view security sensitive files and/or inject content into those files if all of the following are true:

- writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)

Note: other conditions are listed by the vendors, but disputed by researchers.

An attacker could achieve remote code execution if all of the following are true:

- writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)
- application is using Tomcat's file-based session persistence (disabled by default) with the default storage location
- application included a library that may be leveraged in a deserialisation attack (this is the case for many Java applications)

Affected Products

The following versions of Apache Tomcat are affected:

- Apache Tomcat 11.0.0-M1 to 11.0.2 (fixed in 11.0.3 or later)
- Apache Tomcat 10.1.0-M1 to 10.1.34 (fixed in 10.1.35 or later)
- Apache Tomcat 9.0.0.M1 to 9.0.98 (fixed in 9.0.99 or later)

Recommendations

CERT-EU recommends updating the affected products to the latest version.

References

[1] https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq

[2] https://www.rapid7.com/blog/post/2025/03/19/etr-apache-tomcat-cve-2025-24813-what-you-need-to-know/