An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2503180145

NCSC Advisory

Actively Exploited Vulnerability in Apache Tomcat CVE-2025-24813

18th, March 2025

STATUS: TLP:CLEAR

Description

CVE ID: CVE-2025-24813

Published: 2025-03-10

Vendor: Apache Software Foundation

Product: Apache Tomcat

CVSS Score[1]: 5.5

Products Affected

Product	Version
Apache Tomcat	11.0.0-M1 <= 11.0.2
Apache Tomcat	10.1.0-M1 <= 10.1.34
Apache Tomcat	9.0.0.M1 <= 9.0.98

Impact

Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files via write enabled Default Servlet in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0.M1 through 9.0.98.

If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files:

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

[1] https://www.cisa.gov/news-events/bulletins/sb25-076

If all of the following were true, a malicious user was able to perform remote code execution:

- Writes enabled for the default servlet (disabled by default)
- Support for partial PUT (enabled by default)
- Application was using Tomcat's file based session persistence with the default storage location
- Application included a library that may be leveraged in a deserialization attack

Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.98, which fixes the issue.

Common Weakness Enumeration (CWE)[2]: CWE-44 Path Equivalence: 'file.name' (Internal Dot), CWE-502: CWE-502 Deserialization of Untrusted Data

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Apache Software Foundation.

- https://nvd.nist.gov/vuln/detail/CVE-2025-24813
- https://www.cve.org/CVERecord?id=CVE-2025-24813
- https://tomcat.apache.org/security-11.html
- https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq
- http://www.openwall.com/lists/oss-security/2025/03/10/5
- https://github.com/absholi7ly/POC-CVE-2025-24813/blob/main/README.md

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog