

Alert Bulletin

Bulletin N.: 35

Publication Date: 15/04/2026

Subject: Alert 2026-35 Critical Vulnerabilities in Apache Tomcat and one of them affects K8s

Traffic Light Protocol (TLP): White

Affected Product(s):

Product	Affected Versions
Apache Tomcat 9	9.0.13 – 9.0.116
Apache Tomcat 10	10.1.0 – 10.1.53
Apache Tomcat 11	11.0.0 – 11.0.20

Description

Multiple critical vulnerabilities have been reported in Apache Tomcat, highlighting CVE-2026-34486 (CVSS 9.1 – Critical) which allows complete encryption bypass, along with CVE-2026-29146 (High) and CVE-2026-34487 (Kubernetes token leak). These affect exposed Tomcat servers and have been recently patched following a defective fix in intermediate versions.

The main vulnerabilities are detailed below:

- **CVE-2026-34486 (CVSS 9.1 – Critical):** EncryptInterceptor bypass; an attacker manipulates requests to evade encryption completely. Specifically affects 9.0.116, 10.1.53, and 11.0.20.
- **CVE-2026-29146 (CVSS 7.5 – High):** Padding Oracle in EncryptInterceptor allows decrypting sensitive data via adaptive attacks. Covers from 9.0.13 to 9.0.116 (9.x), 10.1.0-M1 to 10.1.53 (10.x), 11.0.0-M1 to 11.0.20 (11.x).
- **CVE-2026-34487 (CVSS 7.5 – High):** is a vulnerability of type **insertion of sensitive information into log files (CWE-532)** in the *cloud membership for clustering* component of Apache Tomcat. When Tomcat is deployed in a Kubernetes cluster and uses this component for cluster member discovery, the code **logs the bearer token of the Kubernetes service account** it uses to talk to the cluster API. That **Kubernetes bearer token** should be treated as a secret (equivalent to a service credential), but ends up written to files like catalina.out or the configured application logs.
- **CVE-2026-29145 (CVSS 9.1 – Critical):** It is a vulnerability in Apache Tomcat and Tomcat Native where, under certain scenarios, **CLIENT_CERT** authentication does not fail as it should when the *soft fail*

option is disabled, allowing **invalid or revoked** client certificates to be accepted and gain access to resources that should be protected by mutual TLS authentication.

These vulnerabilities allow remote code execution (RCE), privilege escalation, and credential theft in production environments. Versions 9.0.116, 10.1.53, and 11.0.20 fixed CVE-2026-29146, but introduced CVE-2026-34486, so it is recommended to immediately update to versions 9.0.117, 10.1.54, or 11.0.21 (or higher).

Given the high level of exposure in cloud environments and Kubernetes deployments, it is recommended to prioritize update tasks on all Apache Tomcat web servers exposed to the Internet.

Solution:

The recommended solution is to update Apache Tomcat to the versions that fix these vulnerabilities: 9.0.117, 10.1.54, or 11.0.21 (or higher), depending on the installed branch.

These versions already include fixes for the encryption issues, token leaks, and authentication bypass, and are available for direct download from the official Apache Tomcat project website, on the download pages for each branch:

- Branch 9.0 <https://tomcat.apache.org/download-90.cgi>
- Branch 10.0 <https://tomcat.apache.org/download-10.cgi>
- Branch 11.0 <https://tomcat.apache.org/download-11.cgi>

Additional information:

- <https://tomcat.apache.org/security.html>
- <https://securityonline.info/apache-tomcat-security-vulnerabilities-encryption-bypass-token-leak/>