

Alert Bulletin

Bulletin N.: 83

Publication Date: 05/08/2026

Subject: Alert 2026-82 Vulnerability in Apache Tomcat actively exploited to distribute SNOWLIGHT malware

Traffic Light Protocol (TLP): White

Affected product(s):

- Apache Tomcat 11.x – versions prior to 11.0.21
- Apache Tomcat 10.x – versions prior to 10.1.54
- Apache Tomcat 9.x – versions prior to 9.0.117

Description

The CISO team confirmed on August 5, 2026 the active exploitation of CVE-2026-34486 in Apache Tomcat, a missing encryption flaw in the clustering component that is being leveraged in AI-enabled campaigns to distribute the SNOWLIGHT loader. Patches were published in April 2026 and apply to the 9.x, 10.x, and 11.x branches.

Apache Tomcat is one of the most widely used Java application servers in the world, broadly deployed in enterprise environments, development platforms, and web services to host applications based on Java Servlets and JSP. On August 5, 2026, CISA added CVE-2026-34486 (CVSS: 7.5 – High) to its Known Exploited Vulnerabilities (KEV) catalog, confirming evidence of real-world active exploitation. The vulnerability, fixed by Apache in April 2026, is being actively leveraged by multiple threat actors, including automated AI-enabled campaigns, to distribute the SNOWLIGHT loader and gain initial access to compromised environments.

• CVE-2026-34486 – Missing Encryption of Sensitive Data in EncryptInterceptor (CVSS: 7.5 – High)

The flaw resides in the inter-node clustering component of Apache Tomcat. The EncryptInterceptor is the mechanism responsible for encrypting the messages exchanged between nodes of a Tomcat cluster using a pre-shared key. A missing encryption of sensitive data vulnerability allows bypassing this component, exposing inter-node traffic and allowing an attacker to intercept, manipulate, or inject messages in the communication between cluster nodes.

In practice, the documented active exploitation uses this vector to introduce the **SNOWLIGHT** loader, an initial access component that facilitates the download and execution of additional payloads on the compromised system, enabling persistence and lateral movement within the affected environment. The

campaign has been attributed to actors employing AI-enabled autonomous hacking techniques, indicating exploitation capabilities at a scale and speed superior to traditional manual campaigns.

Initially, Apache Tomcat fixed in April 2026 the vulnerability **CVE-2026-29146**; you can find information about it in our bulletin:

Alerta 2026-35 Vulnerabilidades Críticas en Apache Tomcat y una de ellas afecta K8s

That vulnerability was from April; it was a *padding oracle*-type issue in the **EncryptInterceptor** component that allowed an attacker to decrypt sensitive information through adaptive attacks against the inter-node encryption mechanism. However, the fixes introduced in versions **9.0.116, 10.1.53, and 11.0.20** were incomplete and resulted in a new critical vulnerability, **CVE-2026-34486**, which enables **complete bypass of encryption** in that same component. To this situation is added **CVE-2026-34487**, which affects the *cloud membership for clustering* mechanism in Kubernetes and exposes in the logs the *bearer token* of the *service account* used by Tomcat to interact with the cluster API.

Taken together, these vulnerabilities show a direct relationship: two of them impact the same cryptographic component and evidence a flawed or insufficient fix, while the third extends the risk toward cloud-native environments by compromising Kubernetes secrets, raising the impact from the inter-node transport layer to the security of the cluster and its associated credentials.

Mitigation

There is no documented temporary mitigation equivalent to applying the patch. As complementary measures while the update is being coordinated:

- Disable or isolate Apache Tomcat inter-node clustering if it is not strictly necessary in the affected environment, thus reducing the attack surface exposed to the EncryptInterceptor.
- Restrict network access to Tomcat clustering ports only to authorized cluster nodes through firewall or network rules.
- Monitor inter-node traffic for anomalous communication patterns between cluster nodes.
- Review Tomcat logs looking for unusual incoming connections or clustering activity from IPs not belonging to the legitimate cluster.

Solution

Update Apache Tomcat to the fixed versions published in April 2026. The update can be performed by downloading the official binary from the Apache Tomcat website and following the manufacturer’s update procedure.

Installed product and version	Fixed version	Update information
Apache Tomcat 11.x – versions prior to 11.0.21	11.0.21	https://tomcat.apache.org/download-11.cgi

Installed product and version	Fixed version	Update information
Apache Tomcat 10.x – versions prior to 10.1.54	10.1.54	https://tomcat.apache.org/download-10.cgi
Apache Tomcat 9.x – versions prior to 9.0.117	9.0.117	https://tomcat.apache.org/download-90.cgi

Additional information:

- The Hacker News – CISA Flags Langflow RCE, Tomcat, and Nginx Central Flaws as Actively Exploited
<https://thehackernews.com/2026/08/cisa-flags-langflow-rce-tomcat-and-n.html>
- CISA – Known Exploited Vulnerabilities Catalog
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- NVD – CVE-2026-34486
<https://nvd.nist.gov/vuln/detail/CVE-2026-34486>
- Apache Tomcat Security Reports
<https://tomcat.apache.org/security.html>
- Apache Tomcat 11 Downloads
<https://tomcat.apache.org/download-11.cgi>
- Apache Tomcat 10 Downloads
<https://tomcat.apache.org/download-10.cgi>
- Apache Tomcat 9 Downloads
<https://tomcat.apache.org/download-90.cgi>
- <https://beaconlab.us/es/publicacion/alerta-2026-35-vulnerabilidades-en-apache-tomcat-y-una-de-ellas-afecta-k8s/>