Boletín de alerta

Boletín Nro.: 83
Fecha de publicación: 05/08/2026
Tema: Alerta 2026-82 Vulnerabilidad en Apache Tomcat explotada activamente para distribuir malware SNOWLIGHT
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Apache Tomcat 11.x – versiones anteriores a 11.0.21
- Apache Tomcat 10.x – versiones anteriores a 10.1.54
- Apache Tomcat 9.x – versiones anteriores a 9.0.117

Descripción

El equipo de CISO confirmó el 5 de agosto de 2026 la explotación activa de CVE□2026□34486 en Apache Tomcat, una falla de cifrado faltante en el componente de clustering que está siendo aprovechada en campañas habilitadas por IA para distribuir el loader SNOWLIGHT. Los parches fueron publicados en abril de 2026 y aplican a las ramas 9.x, 10.x y 11.x.

Apache Tomcat es uno de los servidores de aplicaciones Java más utilizados en el mundo, ampliamente desplegado en entornos empresariales, plataformas de desarrollo y servicios web para alojar aplicaciones basadas en Java Servlets y JSP. El 5 de agosto de 2026, CISA incorporó CVE□2026□34486 (CVSS: 7.5 – Alto) a su catálogo de Known Exploited Vulnerabilities (KEV), confirmando evidencia de explotación activa en el mundo real. La vulnerabilidad, corregida por Apache en abril de 2026, está siendo activamente aprovechada por múltiples actores de amenaza, incluyendo campañas automatizadas habilitadas por inteligencia artificial, para distribuir el loader SNOWLIGHT y ganar acceso inicial a entornos comprometidos.

- **CVE□2026□34486 – Missing Encryption of Sensitive Data en EncryptInterceptor (CVSS: 7.5 – Alto)**

La falla reside en el componente de clustering inter□nodo de Apache Tomcat. El EncryptInterceptor es el mecanismo responsable de cifrar los mensajes que se intercambian entre nodos de un cluster de Tomcat utilizando una clave precompartida. Una vulnerabilidad de cifrado faltante de datos sensibles permite eludir este componente, exponiendo el tráfico inter□nodo y permitiendo a un atacante interceptar, manipular o inyectar mensajes en la comunicación entre nodos del cluster.

En la práctica, la explotación activa documentada utiliza este vector para introducir el loader **SNOWLIGHT**, un componente de acceso inicial que facilita la descarga y ejecución de payloads adicionales en el sistema comprometido, permitiendo persistencia y movimiento lateral dentro del entorno afectado. La

campaña ha sido atribuida a actores que emplean técnicas de hacking autónomo habilitado por IA, lo que indica una capacidad de explotación a escala y velocidad superiores a las campañas manuales tradicionales.

Inicialmente, Apache Tomcat corrigió en abril de 2026 la vulnerabilidad **CVE-2026-29146** pueden encontrar información al respecto en nuestro boletin:

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

Dicha vulnerabilidad era de abril, era un problema de tipo *padding oracle* en el componente **EncryptInterceptor** que permitía a un atacante descifrar información sensible mediante ataques adaptativos contra el mecanismo de cifrado entre nodos. Sin embargo, las correcciones introducidas en las versiones **9.0.116, 10.1.53 y 11.0.20** resultaron incompletas y derivaron en una nueva vulnerabilidad crítica, **CVE-2026-34486**, que permite el **bypass completo del cifrado** en ese mismo componente. A esta situación se suma **CVE-2026-34487**, que afecta el mecanismo de *cloud membership for clustering* en Kubernetes y expone en los logs el *bearer token* de la *service account* utilizada por Tomcat para interactuar con la API del clúster.

En conjunto, estas vulnerabilidades muestran una relación directa: dos de ellas impactan el mismo componente criptográfico y evidencian un fix defectuoso o insuficiente, mientras que la tercera amplía el riesgo hacia entornos cloud-native al comprometer secretos de Kubernetes, elevando el impacto desde la capa de transporte entre nodos hasta la seguridad del clúster y sus credenciales asociadas.

Mitigación

No existe mitigación temporal documentada que sea equivalente a aplicar el parche. Como medidas complementarias mientras se coordina la actualización:

- Deshabilitar o aislar el clustering inter□nodo de Apache Tomcat si no es estrictamente necesario en el entorno afectado, reduciendo así la superficie de ataque expuesta al EncryptInterceptor.
- Restringir el acceso de red a los puertos de clustering de Tomcat únicamente a nodos del cluster autorizados mediante firewall o reglas de red.
- Monitorear tráfico inter□nodo en busca de patrones anómalos de comunicación entre nodos del cluster.
- Revisar logs de Tomcat buscando conexiones entrantes inusuales o actividad de clustering desde IPs no pertenecientes al cluster legítimo.

Solución

Actualizar Apache Tomcat a las versiones corregidas publicadas en abril de 2026. La actualización puede realizarse descargando el binario oficial desde el sitio de Apache Tomcat y siguiendo el procedimiento de actualización del fabricante.

Producto y versión instalada	Versión corregida	Información de actualización
Apache Tomcat 11.x – versiones anteriores a 11.0.21	11.0.21	https://tomcat.apache.org/download-11.cgi
Apache Tomcat 10.x – versiones anteriores a 10.1.54	10.1.54	https://tomcat.apache.org/download-10.cgi
Apache Tomcat 9.x – versiones anteriores a 9.0.117	9.0.117	https://tomcat.apache.org/download-90.cgi

Información adicional:

- The Hacker News – CISA Flags Langflow RCE, Tomcat, and N□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/