Boletín de alerta

Boletín Nro.: 35
Fecha de publicación: 15/04/2026
Tema: Alerta 2026-35 Vulnerabilidades Críticas en Apache Tomcat y una de ellas afecta K8s
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Versiones Afectadas
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

Descripción

Se han reportado múltiples vulnerabilidades críticas en Apache Tomcat, destacando CVE-2026-34486 (CVSS 9.1 – Crítica) que permite bypass completo de cifrado, junto con CVE-2026-29146 (Alta) y CVE-2026-34487 (fuga de tokens Kubernetes). Estas afectan servidores Tomcat expuestos y han sido parcheadas recientemente tras un fix defectuoso en versiones intermedias.

A continuación se detallen los vulnerabilidades principales:

- **CVE-2026-34486 (CVSS 9.1 – Crítica)**: Bypass del EncryptInterceptor; un atacante manipula requests para evadir cifrado por completo. Afecta específicamente 9.0.116, 10.1.53 y 11.0.20.
- **CVE-2026-29146 (CVSS 7.5 – Alta)**: Padding Oracle en EncryptInterceptor permite descifrar datos sensibles vía ataques adaptativos. Cubre desde 9.0.13 hasta 9.0.116 (9.x), 10.1.0-M1 hasta 10.1.53 (10.x), 11.0.0-M1 hasta 11.0.20 (11.x).
- **CVE-2026-34487 (CVSS 7.5 – Alta)**: es una vulnerabilidad de tipo **inserción de información sensible en archivos de log (CWE-532)** en el componente de *cloud membership for clustering* de Apache Tomcat. Cuando Tomcat está desplegado en un clúster de Kubernetes y usa este componente para el descubrimiento de miembros del clúster, el código **registra en los logs el bearer token del service account de Kubernetes** que utiliza para hablar con la API del cluster. Ese **Kubernetes bearer token** debería tratarse como secreto (equivalente a una credencial de servicio), pero termina escrito en ficheros como catalina.out o los logs configurados de la aplicación.

- **CVE-2026-29145 (CVSS 9.1 – Crítica)**: Es una vulnerabilidad en Apache Tomcat y Tomcat Native donde, bajo ciertos escenarios, la autenticación **CLIENT_CERT** no falla como debería cuando la opción de *soft fail* está deshabilitada, lo que permite que certificados de cliente **inválidos o revocados** sean aceptados y consigan acceso a recursos que deberían estar protegidos por autenticación mutua TLS.

Estas vulnerabilidades permiten la ejecución remota de código (RCE), la escalada de privilegios y el robo de credenciales en entornos productivos. Las versiones 9.0.116, 10.1.53 y 11.0.20 corregían la CVE-2026-29146, pero introdujeron la CVE-2026-34486, por lo que se recomienda actualizar de forma inmediata a las versiones 9.0.117, 10.1.54 o 11.0.21 (o superiores).

Dado el alto nivel de exposición en entornos cloud y despliegues sobre Kubernetes, se recomienda priorizar las tareas de actualización en todos los servidores web Apache Tomcat expuestos a Internet.

Solución:

La solución recomendada consiste en actualizar Apache Tomcat a las versiones que corrigen estas vulnerabilidades: 9.0.117, 10.1.54 o 11.0.21 (o superiores), según la rama que se tenga instalada.

Estas versiones ya incorporan los fixes para los problemas de cifrado, fuga de tokens y bypass de autenticación, y están disponibles para su descarga directa desde el sitio oficial del proyecto Apache Tomcat, en las páginas de descargas de cada rama:

- Rama 9.0 **https://tomcat.apache.org/download-90.cgi**
- Rama 10.0 **https://tomcat.apache.org/download-10.cgi**
- Rama 11.0 https://tomcat.apache.org/download-11.cgi

Información adicional:

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