Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

APACHE TOMCAT EN LA MIRA: VULNERABILIDAD RCE CRÍTICA EN EXPLOTACIÓN

18/ 03 / 2025

CONTENIDO

INTRODUCCIÓN

Apache Tomcat se encuentra en el centro de atención debido a una vulnerabilidad de ejecución remota de código (RCE) que está siendo activamente explotada. Esta falla representa un riesgo significativo para las empresas que dependen de este servidor web, ya que los atacantes pueden comprometer sistemas y acceder a información crítica. Ante esta amenaza, es crucial que las organizaciones actúen rápidamente para proteger sus infraestructuras.

APACHE TOMCAT EN LA MIRA: VULNERABILIDAD RCE CRÍTICA EN EXPLOTACIÓN

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_03_18_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	18/03/2025
Es día cero (0 day):	No

RESUMEN

Apache Tomcat, uno de los servidores web más utilizados en aplicaciones empresariales, enfrenta una vulnerabilidad de ejecución remota de código (RCE) que está siendo activamente explotada por ciberdelincuentes. Esta falla permite a los atacantes ejecutar código malicioso de forma remota, comprometiendo sistemas y poniendo en riesgo datos sensibles. Su gravedad la convierte en una amenaza crítica, especialmente en entornos corporativos donde la seguridad de la infraestructura es esencial.

¿Qué es una vulnerabilidad RCE?

La ejecución remota de código (RCE) permite a un atacante ejecutar comandos en un servidor vulnerable sin autenticación, lo que facilita el robo de información, la manipulación de archivos o la instalación de malware.

En el caso de Apache Tomcat, la vulnerabilidad CVE-2025-24813 afecta la implementación del método PUT parcial, lo que puede derivar en divulgación de información, corrupción de datos y, en ciertos casos, ejecución remota de código.

Detalles Técnicos

La falla radica en el manejo de archivos temporales cuando se usa PUT parcial. Un atacante podría aprovechar esta debilidad para acceder a archivos sensibles, sobrescribir archivos críticos o ejecutar código remoto si la aplicación afectada usa persistencia de sesión basada en archivos y una biblioteca vulnerable a ataques de deserialización.

Para que esta vulnerabilidad sea explotable, deben cumplirse ciertas condiciones, como tener habilitada la escritura en el servlet predeterminado y el uso de PUT parcial.

Explotación Activa

Los atacantes están escaneando servidores en busca de versiones vulnerables de Tomcat. Una vez identificados, explotan la falla con ataques automatizados, enviando solicitudes maliciosas para manipular PUT parcial y ejecutar código o acceder a información crítica.

Los impactos incluyen robo de información confidencial, corrupción de archivos, instalación de malware y movimiento lateral dentro de la red.

Versiones Afectadas y Solución

Versiones vulnerables:

- Apache Tomcat 11.0.0-M1 a 11.0.2
- Apache Tomcat 10.1.0-M1 a 10.1.34
- Apache Tomcat 9.0.0.M1 a 9.0.98

Versiones seguras:

- Apache Tomcat 11.0.3 o posterior

- Apache Tomcat 10.1.35 o posterior
- Apache Tomcat 9.0.99 o posterior

Impacto de la vulnerabilidad

La explotación de esta vulnerabilidad puede generar pérdida de datos, accesos no autorizados, interrupción de servicios y propagación de malware dentro de la red corporativa. Las empresas que dependen de Apache Tomcat deben actuar de inmediato para mitigar el riesgo.

Recomendaciones

1. **Correos maliciosos y phishing:** Los atacantes pueden enviar correos falsos simulando ser Apache o equipos de TI para robar credenciales o distribuir malware. Se recomienda verificar remitentes, evitar enlaces sospechosos y capacitar a los empleados en detección de phishing.
2. **Descargas comprometidas:** Los ciberdelincuentes pueden distribuir versiones alteradas de Tomcat mediante sitios falsos o infectados. Para evitarlo, es esencial descargar software solo del sitio oficial, verificar firmas digitales y probar actualizaciones en entornos controlados.
3. **Suplantación de identidad para robo de credenciales:** Los atacantes pueden hacerse pasar por soporte técnico para obtener accesos. No se deben compartir credenciales y se recomienda activar autenticación multifactor y monitorear accesos sospechosos.
4. **Explotación de herramientas maliciosas:** El malware puede ocultarse en scripts o bibliotecas alteradas. Se deben descargar archivos solo desde fuentes verificadas, analizarlos antes de ejecutarlos y revisar dependencias del sistema.
5. **Mantener Apache Tomcat actualizado:** Aplicar las versiones seguras es la mejor mitigación. Se recomienda monitorear avisos de seguridad, actualizar de inmediato y automatizar el proceso de actualización cuando sea posible.

NOTICIA COMPLETA

https://devel.group/blog/apache-tomcat-en-la-mira-vulnerabilidad-rce-critica-en-explotacion/

CONTACTOS DE SOPORTE

Correo electrónico: info@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/