Una reciente vulnerabilidad de seguridad en Apache Tomcat ha comenzado a ser explotada activamente después de que se publicara un exploit de prueba de concepto (PoC) solo 30 horas después de su divulgación pública.

La falla, identificada como CVE-2025-24813, afecta las siguientes versiones:

- 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

El problema está relacionado con la ejecución remota de código o la exposición de información sensible bajo ciertas condiciones:

- Escritura habilitada para el servlet predeterminado (deshabilitado por defecto).
- Soporte para solicitudes parciales PUT (habilitado por defecto).
- Una URL objetivo para archivos sensibles que esté dentro de una subcarpeta de una URL de carga pública.
- Conocimiento previo por parte del atacante sobre los nombres de los archivos sensibles que se están subiendo.
- Los archivos sensibles también son subidos mediante solicitudes parciales PUT.

Si se explota con éxito, un atacante podría acceder a archivos sensibles o modificar su contenido enviando una solicitud PUT.

Además, si se cumplen las siguientes condiciones, el atacante podría ejecutar código remoto:

- Escritura habilitada en el servlet predeterminado.
- Soporte para solicitudes parciales PUT activado.
- La aplicación usa almacenamiento de sesiones basado en archivos con la ubicación predeterminada de Tomcat.
- La aplicación incluye una biblioteca vulnerable a ataques de deserialización.

Explotación activa y riesgos

Según un aviso de los desarrolladores de Apache, la vulnerabilidad ha sido corregida en Tomcat 9.0.99, 10.1.35 y 11.0.3.

Sin embargo, la empresa de ciberseguridad Wallarm ha advertido que los intentos de explotación ya están en curso. Según sus análisis, el ataque se basa en el mecanismo de persistencia de sesiones de Tomcat y su soporte para solicitudes PUT parciales.

El exploit se desarrolla en dos pasos:

1. El atacante sube un archivo de sesión de Java serializado mediante una solicitud PUT.
2. Luego, ejecuta el código malicioso enviando una solicitud GET que referencia el ID de sesión malicioso.

En términos más simples, el ataque implica enviar una carga útil de Java codificada en Base64 a la carpeta de almacenamiento de sesiones de Tomcat. Posteriormente, al referenciar este archivo mediante una solicitud GET con el JSESSIONID correspondiente, se ejecuta el código malicioso.

Además, Wallarm advierte que esta vulnerabilidad es fácil de explotar y no requiere autenticación, siempre que Tomcat utilice almacenamiento de sesiones basado en archivos. También señala que los atacantes podrían evolucionar su enfoque para:

- Subir archivos JSP maliciosos.
- Modificar configuraciones del servidor.
- Insertar puertas traseras fuera del almacenamiento de sesiones.

Recomendaciones

Los administradores que utilicen versiones afectadas de Tomcat deben actualizar sus servidores de inmediato para prevenir posibles ataques y mitigar riesgos de seguridad.