Boletín de alerta

Boletín Nro.: 94
Fecha de publicación: 29/10/2025
Tema: Alerta 2025-94 Vulnerabilidades importantes en Apache Tomcat
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Apache Tomcat:

- Tomcat 11.0.0-M1 a 11.0.10
- Tomcat 10.1.0-M1 a 10.1.44
- Tomcat 9.0.0.M11 a 9.0.108

Descripción

Se han publicado 3 vulnerabilidades importante que afecta al producto Apache Tomcat, CVE-2025-55752, CVE-2025-55754 y CVE-2025-61795 que afectan a las versiones de Tomcat 9, 10 y 11. La más grave, CVE-2025-55752, podría provocar la ejecución remota de código (RCE) si se cumplen condiciones específicas.

El problema más crítico, CVE-2025-55752 con score CVSSv3 7.5, se debe a una regresión en el manejo de la reescritura de URL de Tomcat. Según el reporte, *la corrección del error 60013 introdujo una regresión donde la URL reescrita se normalizaba antes de ser decodificada. Esto abrió la posibilidad de que, para las reglas de reescritura que modifican los parámetros de consulta en la URL, un atacante pudiera manipular el URI de la solicitud para eludir las restricciones de seguridad, incluida la protección para /WEB-INF/ y /META-INF/*

Esta vulnerabilidad podría permitir a los atacantes eludir los controles de acceso y, bajo ciertas configuraciones, cargar archivos maliciosos a través de solicitudes HTTP PUT, lo que podría eventualmente dar lugar a la ejecución remota de código. Sin embargo, Apache señala que la explotación es improbable en configuraciones estándar, ya que "las *solicitudes PUT normalmente se limitan a usuarios de confianza y se considera improbable que las solicitudes PUT se habiliten junto con una reescritura que manipule el URI*".

Otra vulnerabilidad, CVE-2025-55754 con score CVSSv3 5.3, afecta a las instancias de Tomcat que se ejecutan en entornos Windows con consolas que admiten secuencias de escape ANSI.

La tercera vulnerabilidad, CVE-2025-61795 con score CVSSv3 5.3, podría causar una condición de denegación de servicio (DoS) durante las cargas de archivos multipartes.

Solución:

Los usuarios deben actualizar a Apache Tomcat 11.0.12, 10.1.47 o 9.0.110 para corregir estas vulnerabilidades.

https://tomcat.apache.org/upgrading.html

Información adicional:

- https://lists.apache.org/thread/38vqp0v1fg4gr8c6lvm15wj6k67hxzxd
- https://securityonline.info/apache-tomcat-patches-url-rewrite-bypass-cve-2025-55752-risking-rce-and-console-ansi-injection/