La Apache Software Foundation (ASF) ha publicado una actualización de seguridad para resolver una vulnerabilidad significativa en su software de servidor Tomcat que, bajo ciertas circunstancias, podría permitir la ejecución remota de código (RCE).

Esta vulnerabilidad, identificada como CVE-2024-56337, se describe como una mitigación parcial de la falla CVE-2024-50379 (puntuación CVSS: 9.8), otro problema crítico de seguridad en el mismo producto que fue solucionado previamente el 17 de diciembre de 2024.

> *«Los usuarios que utilicen Tomcat en sistemas de archivos que no diferencian entre mayúsculas y minúsculas, con el servlet predeterminado configurado para permitir escritura (es decir, el parámetro de inicialización `readonly` ajustado a `false` en lugar del valor predeterminado), podrían necesitar ajustes adicionales en la configuración para proteger completamente contra CVE-2024-50379, dependiendo de la versión de Java que estén ejecutando con Tomcat»,* advirtieron los encargados del proyecto en un comunicado reciente.

Ambos fallos corresponden a vulnerabilidades de condiciones de carrera de tipo «verificación y uso» (TOCTOU) que pueden conducir a la ejecución de código en sistemas de archivos insensibles a las diferencias entre mayúsculas y minúsculas cuando el servlet predeterminado está habilitado para escritura.

> *«La lectura y carga simultánea de un mismo archivo bajo presión puede evadir las verificaciones de sensibilidad de mayúsculas y minúsculas de Tomcat, provocando que un archivo cargado sea interpretado como un JSP, lo que permite la ejecución remota de código»,* explicó Apache en su advertencia sobre CVE-2024-50379.

## Versiones afectadas por CVE-2024-56337

Las versiones de Apache Tomcat que presentan esta vulnerabilidad son las siguientes:

- Apache Tomcat 11.0.0-M1 a 11.0.1 (corregido en 11.0.2 o posterior).
- Apache Tomcat 10.1.0-M1 a 10.1.33 (corregido en 10.1.34 o posterior).
- Apache Tomcat 9.0.0.M1 a 9.0.97 (corregido en 9.0.98 o posterior).

## Cambios necesarios según la versión de Java

Dependiendo de la versión de Java utilizada, los usuarios deben realizar los siguientes ajustes:

- Java 8 o Java 11: Configurar la propiedad del sistema `sun.io.useCanonCaches` a `false` (por defecto, está en `true`).
- Java 17: Asegurarse de que la propiedad del sistema `sun.io.useCanonCaches` esté en `false` (por defecto, ya se encuentra en `false`).
- Java 21 y versiones posteriores: No es necesario realizar ningún cambio, ya que esta propiedad del sistema ha sido eliminada.

La ASF reconoció la contribución de los investigadores de seguridad Nacl, WHOAMI, Yemoli y Ruozhi por descubrir y reportar ambas vulnerabilidades. También agradeció al equipo KnownSec 404 por identificar CVE-2024-56337 de forma independiente y proporcionar un código de prueba de concepto (PoC).

Por otro lado, la Zero Day Initiative (ZDI) ha revelado un fallo crítico en Webmin (CVE-2024-12828, puntuación CVSS: 9.9) que podría permitir a atacantes remotos autenticados ejecutar código arbitrario.

> *«El problema reside en el manejo de solicitudes CGI. El fallo ocurre debido a la falta de validación adecuada de una cadena proporcionada por el usuario antes de usarla en una llamada al sistema. Un atacante podría explotar esta vulnerabilidad para*

> *ejecutar código con privilegios de root»*, explicó la ZDI.