BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-71
Fecha de publicación: 27/12/2024
Tema: Vulnerabilidad RCE critica en Apache Tomcat
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- 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)

Además, los usuarios deben realizar los siguientes cambios de configuración según la versión de Java que se esté ejecutando:

- Java 8 o Java 11: establezca explícitamente la propiedad del sistema sun.io.useCanonCaches en False (el valor predeterminado es True)
- Java 17: Establezca la propiedad del sistema sun.io.useCanonCaches en False, si ya está configurada (el valor predeterminado es False)
- Java 21 y posteriores: no se requiere ninguna acción, ya que se ha eliminado la propiedad del sistema

Descripción

Se ha publicado una vulnerabilidad crítica en su software de servidor Tomcat que podría provocar ejecución remota de código (RCE) bajo ciertas condiciones. La vulnerabilidad, identificada como CVE-2024-56337 , ha sido descrita como una mitigación incompleta para CVE-2024-50379 con puntuación CVSS: 9.8, otra falla de seguridad crítica en el mismo producto que se abordó previamente el 17 de diciembre de 2024.

Ambas fallas son vulnerabilidades de condición de carrera de tiempo de verificación y tiempo de uso (TOCTOU) que podrían resultar en la ejecución de código en sistemas de archivos que no distinguen entre mayúsculas y minúsculas cuando el servlet predeterminado está habilitado para escritura.

"La lectura y carga simultáneas del mismo archivo pueden eludir las comprobaciones de distinción entre mayúsculas y minúsculas de Tomcat y provocar que un archivo cargado se trate como un JSP, lo que lleva a la ejecución remota de código", señaló Apache en una alerta para CVE-2024-50379.

Solución

El equipo de Apache Software Foundation ha publicado parches de seguridad las mismas son:

- 11.0.2
- 10.1.34
- 9.0.98

Tomcat 11.0.3, 10.1.35 y 9.0.99 en adelante incluirán comprobaciones de que sun.io.useCanonCaches esté configurado correctamente antes de permitir que el servlet predeterminado esté habilitado para escritura en un sistema de archivos que no distinga entre mayúsculas y minúsculas. Tomcat también configurará sun.io.useCanonCaches como falso de manera predeterminada cuando sea posible.

Información adicional:

- https://thehackernews.com/2024/12/apache-tomcat-vulnerability-cve-2024.html
- https://www.cve.org/CVERecord?id=CVE-2024-56337
- https://tomcat.apache.org/security-10.html
- https://lists.apache.org/thread/b2b9qrgjrz1kvo4ym8y2wkfdvwoq6qbp

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com