BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-40
Fecha de publicación: 24/09/2024
Tema: CVE-2024-38286 Apache Tomcat DoS
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Apache Tomcat 9.0.13 - 9.0.89, 10.1.0 M1 – 10.1.24 y 11.0.0 M1– 11.0.0 M20

Descripción

Se ha descubierto una vulnerabilidad crítica en Apache Tomcat que afecta a las versiones hasta 9.0.89, 10.1.24 y 11.0.0-M20. Esta vulnerabilidad, conocida como CVE-2024-38286, está relacionada con el componente TLS Handshake Handler y permite un consumo excesivo de recursos. El problema, clasificado bajo la CWE-400 (Exhaustión de Recursos), ocurre debido a una mala gestión de los recursos limitados durante el proceso de handshake TLS, lo que puede llevar al agotamiento de la memoria y afectar la disponibilidad del servicio.

El ataque puede ser lanzado remotamente, sin necesidad de autenticación, y es relativamente sencillo de explotar. Sin embargo, aún no se han revelado detalles técnicos ni hay un exploit disponible públicamente. El impacto principal es la disponibilidad del servidor, lo que puede provocar interrupciones en aplicaciones y servicios críticos que dependan de Apache Tomcat.

La vulnerabilidad afecta a las siguientes versiones de Apache Tomcat:

- Apache Tomcat 11.0.0-M1 a 11.0.0-M20
- Apache Tomcat 10.1.0-M1 a 10.1.24
- Apache Tomcat 9.0.13 a 9.0.89

El ataque se clasifica bajo la técnica T1499 según MITRE ATT&CK, asociada a ataques de denegación de servicio (DoS)..

Solución

La Apache Software Foundation ha emitido un aviso de seguridad instando a todos los usuarios de las versiones afectadas de Apache Tomcat a actualizar a versiones más seguras. Las actualizaciones corregidas están disponibles en el sitio oficial de Apache Tomcat.

Versiones recomendadas:

- Para Apache Tomcat 11, actualizar a la versión 11.0.0-M21 o posterior.
- Para Apache Tomcat 10.1, actualizar a la versión 10.1.25 o posterior.
- Para Apache Tomcat 9.0, actualizar a la versión 9.0.90 o posterior.

Estas actualizaciones eliminan la vulnerabilidad, mitigando el riesgo de ataques que pueden provocar la caída del servidor debido a un consumo excesivo de memoria. Es altamente recomendable que los administradores de sistemas implementen estas actualizaciones de inmediato para evitar interrupciones operativas y garantizar la disponibilidad de los servicios.

Información adicional:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-38286
- https://vuldb.com/?id.278287
- https://x.com/the_yellow_fall/status/1838395548187136027

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com