BEACON LAB
C S I R T

CYBOLT
Security Innovation

# Boletín de Alerta

Boletín Nro.: 2024-24
Fecha de publicación: 03/09/2024
Tema: Vulnerabilidad RCE crítica en Jenkins
Traffic Light Protocol (TLP): White


## Producto(s) afectado:

- Jenkins 2.470 y anteriores,
- Jenkins LTS 2.452.3 y anteriores

## Descripción

Se ha reportado una vulnerabilidad critica en Jenkins, una herramienta ampliamente utilizada para automatizar tareas de desarrollo de software, denominada con el CVE-2024-43044 con un scoring CVSSv3 de 8.8, permite a los agentes de Jenkins leer archivos arbitrarios del controlador.

Esta vulnerabilidad surge de una falla en el método ClassLoaderProxy#fetchJar, que no restringe las rutas de archivo que los agentes pueden solicitar al controlador. Este descuido puede potencialmente escalar a una ejecución de código remoto (RCE) si un atacante secuestra un agente de Jenkins.

Esta vulnerabilidad se puede explotar mediante varios métodos, incluido el uso de secrets del agente para establecer conexiones no autorizadas o conectarse a un proceso Remoting en ejecución.

Una técnica de explotación notable implica falsificar una cookie de “recuérdame” para una cuenta de administrador, lo que permite a los atacantes obtener acceso a la consola de scripts de Jenkins y ejecutar comandos. Esta técnica requiere leer archivos específicos para crear una cookie válida, aprovechando la vulnerabilidad para leer archivos binarios y el contenido completo de archivos.

Actualmente, se ha publicado un PoC (Prueba de Concepto) de esta vulnerabilidad. La disponibilidad de un PoC para una vulnerabilidad incrementa el riesgo de ataques en tu empresa, ya que facilita a los atacantes la explotación de la falla. Esto requiere una acción urgente para mitigar la vulnerabilidad, como aplicar parches y revisar políticas de seguridad.

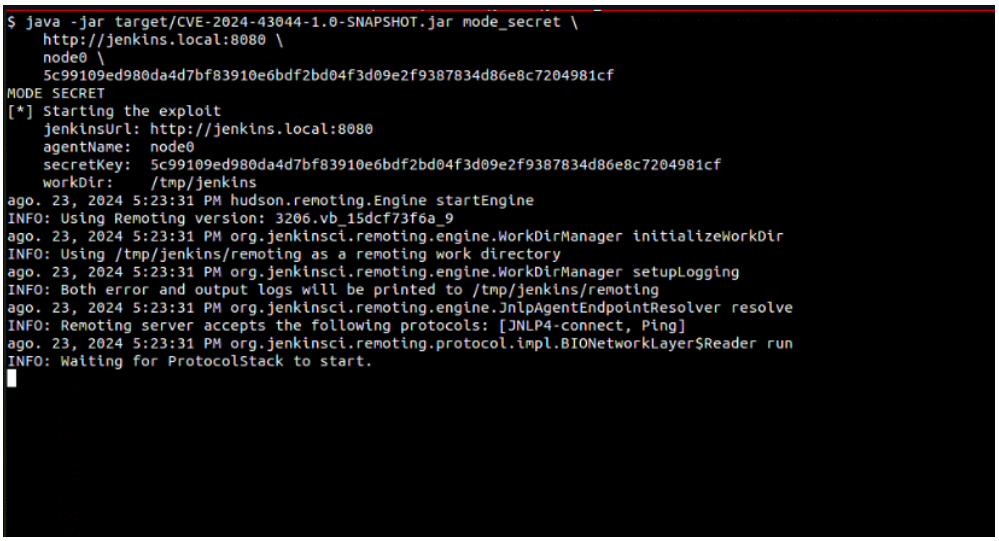


*Figura 1 Imagen de la ejecución del PoC para luego tener acceso a consola del servidor.*

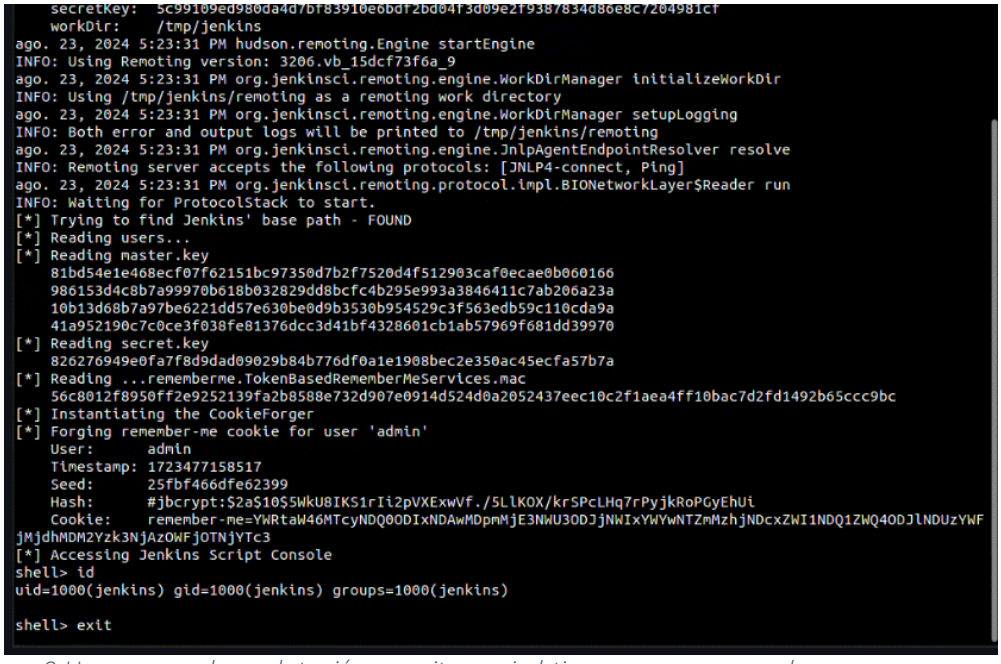


*Figura 2 Una vez que la explotación es exitosa, si obtiene acceso a consola.*

## Solución

El equipo de Jenkins ha publicado un parche para solucionar este problema, introduciendo un validador y propiedades del sistema Java para controlar la funcionalidad *fetchJar*.

La biblioteca Remoting en Jenkins 2.471, LTS 2.452.4, LTS 2.462.1 ahora envía contenidos de archivos jar con solicitudes Channel#preloadJar, el único caso de uso de ClassLoaderProxy#fetchJar en agentes, de modo que los agentes ya no necesitan solicitar contenidos de archivos JAR a los controladores.

Estas medidas tienen como objetivo restringir el acceso no autorizado a los archivos mediante la validación de las URL y el rechazo de los archivos JAR no autorizados.

Para obtener las actualizaciones con el parche proveidas por Jenkins (versiones >= LTS 2.462.1 ) puede dirigirse al siguiente enlance:

https://www.jenkins.io/download/

## Información adicional:

- https://www.jenkins.io/security/advisory/2024-08-07/#SECURITY-3430
- https://nvd.nist.gov/vuln/detail/CVE-2024-43044

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com