	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°023	Fecha: 26-01-2024
		Página: 7 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica de ejecución remota de código en Jenkins		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo ejecución remota de código en la interfaz de línea de comandos incorporada (CLI) integrada de Jenkins. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto obtener claves criptográficas y ejecutar código arbitrario.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-23897 de tipo ejecución remota de código en la CLI integrada de Jenkins, existe debido a que el analizador de comandos (la biblioteca args4j) tiene una característica en la que un carácter '@' seguido de una ruta de archivo en un argumento se reemplaza con el contenido del archivo. Esto permite a los atacantes leer archivos arbitrarios en el sistema de archivos del controlador Jenkins utilizando la codificación de caracteres predeterminada del proceso del controlador Jenkins. Un atacante simplemente necesitaría encontrar “un comando que tome un número arbitrario de argumentos y los muestre al usuario” y explotar la vulnerabilidad para acceder al contenido del archivo desde el que se completan los argumentos.

A. Productos afectados:

- Jenkins versión 2.441 y anteriores y a LTS 2.426.2 y anteriores.

Las últimas versiones de Jenkins también resuelven dos errores de alta gravedad, incluido un error de secuestro de WebSocket entre sitios (CSWSH) que conduce a la ejecución de comandos CLI y un archivo arbitrario leído en el complemento Git Server que tiene un impacto similar al de CVE-2024-23897, pero requiere autenticación para su explotación.

Por otro lado, Jenkins también anunció parches para varias vulnerabilidades de gravedad media y baja en el servidor de automatización de código abierto, así como correcciones para múltiples vulnerabilidades de alta gravedad en varios complementos, pero advirtió que CVE-2024-23904, una falla del complemento de comando de registro similar a CVE-2024-23897, permanece sin parchear.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la versión de Jenkins 2.442 y LTS 2.426.3 que aborda esta vulnerabilidad.
- Desactivar la función del analizador de comandos. Si no es posible actualizar a las últimas versiones, se recomienda a los administradores que deshabiliten el acceso a la CLI de Jenkins, lo que evita la explotación por completo, pero solo como solución temporal.

Fuente de Información:	• hxxps://www.sonarsource.com/blog/excessive-expansion-uncovering-critical-security-vulnerabilities-in-jenkins/ • hxxps://www.securityweek.com/critical-jenkins-vulnerability-leads-to-remote-code-execution/ • hxxps://www.jenkins.io/security/advisory/2024-01-24/