BOLETÍN DE ALERTA

Boletín Nro.: 2024-07
Fecha de publicación: 29/01/2024
Tema: Vulnerabilidades en Jenkins permiten ejecución remota de código RCE

Productos afectados:

- Versiones Jenkins 2.441, LTS 2.426.2 y anteriores.

Descripción:

Jenkins ha emitido un reporte sobre una vulnerabilidad de severidad crítica que afecta al núcleo del sistema de las versiones 2.441 y 2.426.2, que permitirían la ejecución remota de código (*RCE*), se ha asignado el identificador CVE-204-23897 para la misma. La vulnerabilidad se produce en la biblioteca args4j es utilizada para analizar argumentos y opciones de comandos en el controlador Jenkins cuando son solicitados a través de CLI. Este analizador de comandos tiene una característica que reemplaza un '@carácter' seguido de una ruta de archivo en un argumento con el contenido del archivo 'expandAtFiles'. Además el fabricante Jenkins ha reportado otra vulnerabilidad de severidad alta, identificada como CVE-2024-23898, del tipo *Cross-site WebSocket hijacking* , la cual permitiría a un actor malicioso ejecutar comandos arbitrarios en el ambiente CLI a través del engaño a un usuario de la aplicación, para que éste acceda a un enlace malicioso a través de técnicas de ingeniería social como enlaces de phishing dirigido al usuario.

Impacto:

La explotación de estas vulnerabilidades podría permitir a un actor malicioso la ejecución remota de código (*RCE*) en sistemas afectados. Actualmente existe una Prueba de Concepto (PoC) publicada para la CVE-2024-23897.

Recomendación:

Se recomienda actualizar a las últimas versiones Jenkins 2.442, LTS 2.426.3 desde su página oficial.

O, como alternativa, si no puede realizar la actualización, puede deshabilitar configurando el *Java system property hudson.cli.CLICommand.allowAtSyntax* a *true.* Realizar esta configuración no es aconsejable en cualquier red accesible por usuarios que no sean administradores de Jenkins.

Información adicional:

- https://www.jenkins.io/security/advisory/2024-01-24/
- https://nvd.nist.gov/vuln/detail/CVE-2024-23897
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/lectura-arbitraria-de-archivos-en-jenkins

- https://www.bleepingcomputer.com/news/security/exploits-released-for-critical-jenkins-rce-flaw-patch-now/