Los actores maliciosos están aprovechando una vulnerabilidad crítica de seguridad recientemente corregida que afecta a JFrog Artifactory, apenas unos días después de que el fallo fuera divulgado públicamente, según un informe de watchTowr.

La vulnerabilidad identificada corresponde a CVE-2026-82329 (puntuación CVSS: 9.8) y consiste en una omisión del mecanismo de autenticación que podría permitir obtener acceso administrativo en Artifactory.

"JFrog Artifactory presenta una debilidad en su mecanismo de autenticación que, bajo la configuración predeterminada, puede permitir que un atacante no autenticado con acceso a la red obtenga privilegios administrativos", señala la descripción de la vulnerabilidad publicada en CVE.org.

JFrog solucionó el problema mediante la versión 7.161.20 de Artifactory, lanzada el 28 de agosto de 2026. Las versiones afectadas son las siguientes:

7.161.0 > 7.161.19
7.146.0 > 7.146.36
7.133.0 > 7.133.28
7.125.0 > 7.125.19
7.117.0 > 7.117.27
7.111.4 > 7.111.21

"Afecta las configuraciones predeterminadas, no requiere autenticación ni interacción del usuario", afirmó el CEO de Vercel, Guillermo Rauch, en una publicación de LinkedIn. "Es una bomba de RCE porque Artifactory almacena binarios, por lo que básicamente se puede contaminar todo; sin embargo, una escalada de privilegios administrativos puede provocar daños incluso mayores".

El origen del problema se encuentra en JFrog Access, componente encargado de emitir y validar credenciales. "Las instancias que no tienen configurada una clave de unión adicional reciben una clave de unión 'fantasma' que los atacantes pueden aprovechar para falsificar el

acceso y generar credenciales con privilegios de administrador", explicó Yordan Ganchev, especialista principal en inteligencia de amenazas de watchTowr, en una declaración.

Ganchev también señaló que, desde el 1 de septiembre de 2026, los actores de amenazas han comenzado a explotar activamente la vulnerabilidad para crear tokens administrativos y obtener información sobre usuarios, grupos, conjuntos de credenciales y topologías de acceso federado.

"El paso desde la divulgación hasta la explotación en escenarios reales se produjo con una eficiencia preocupante", añadió Ganchev. "Cualquiera que haya seguido esta situación sabe lo que viene después: las cosas probablemente empeorarán".

"Cuando los atacantes consiguen acceso administrativo a un sistema central que forma parte de la cadena de suministro de software, pueden hacer aquello en lo que cualquier equipo de ingeniería destaca: desarrollar, enviar y distribuir software rápidamente. A partir de ahí, podrían manipular las canalizaciones de compilación, desplazarse lateralmente hacia sistemas de producción y, potencialmente, distribuir modificaciones maliciosas a los clientes".

Se recomienda a las organizaciones que utilizan versiones autogestionadas de JFrog Artifactory instalar cuanto antes los parches correspondientes en los sistemas expuestos a Internet. Asimismo, deberían revisar los registros de auditoría, cambiar las credenciales que pudieran haber quedado expuestas y analizar los sistemas conectados para detectar modificaciones maliciosas o posibles mecanismos de acceso persistente.