Actores maliciosos han iniciado la explotación activa de una vulnerabilidad crítica recientemente revelada que afecta a Atlassian Confluence Data Center y Confluence Server, apenas tres días después de su divulgación pública.

Identificada como CVE-2023-22527 (puntuación CVSS: 10.0), la vulnerabilidad impacta versiones desactualizadas del software, permitiendo a atacantes no autenticados lograr la ejecución remota de código en instalaciones susceptibles.

Este fallo afecta a las versiones 8 de Confluence Data Center y Server lanzadas antes del 5 de diciembre de 2023, así como la versión 8.4.5.

Sin embargo, en pocos días desde que la falla se hizo pública, se han registrado casi 40,000 intentos de explotación dirigidos a CVE-2023-22527 en la naturaleza, tan temprano como el 19 de enero, provenientes de más de 600 direcciones IP únicas, según informaron tanto la Shadowserver Foundation como el DFIR Report.

La actividad actual se limita a *«intentos de llamadas de prueba y ejecución de 'whoami'»,* sugiriendo que los actores de amenazas están buscando oportunidades para escanear servidores vulnerables con fines de explotación futura.

La mayoría de las direcciones IP de los atacantes son de Rusia (22,674), seguidas por Singapur, Hong Kong, Estados Unidos, China, India, Brasil, Taiwán, Japón y Ecuador.

Hasta el 21 de enero de 2024, se ha descubierto que más de 11,000 instancias de Atlassian son accesibles a través de Internet, aunque actualmente no se sabe cuántas de ellas son vulnerables a CVE-2023-22527.

> *«CVE-2023-22527 es una vulnerabilidad crítica en Atlassian Confluence Server y Data Center. Esta vulnerabilidad tiene el potencial de permitir que atacantes no autenticados inserten expresiones OGNL en la instancia de Confluence, lo que posibilita la ejecución de código arbitrario y comandos del sistema»,* señalaron los

> investigadores de ProjectDiscovery Rahul Maini y Harsh Jaiswal en un análisis técnico de la falla.