Un fallo crítico de seguridad recientemente descubierto que afecta a la plataforma de redes en la nube Aviatrix Controller está siendo activamente explotado para instalar puertas traseras y mineros de criptomonedas.

La firma de seguridad en la nube Wiz ha informado que está atendiendo *«varios incidentes»* relacionados con el uso malintencionado de la vulnerabilidad CVE-2024-50603 (calificación CVSS: 10.0), un error de máxima gravedad que permite la ejecución remota de código sin necesidad de autenticación.

En términos simples, si esta vulnerabilidad es explotada con éxito, los atacantes pueden ejecutar comandos maliciosos en el sistema operativo debido a que ciertos puntos finales de la API no validan correctamente las entradas proporcionadas por los usuarios. Las versiones 7.1.4191 y 7.2.4996 han solucionado este problema.

El investigador de seguridad Jakub Korepta, de la empresa polaca de ciberseguridad Securing, identificó y reportó esta vulnerabilidad. Desde entonces, se ha publicado un exploit de prueba de concepto (PoC) para demostrar la vulnerabilidad.

Según los datos recopilados por Wiz, alrededor del 3% de los entornos empresariales en la nube utilizan Aviatrix Controller, y de estos, el 65% presentan rutas de movimiento lateral que podrían permitir acceder a permisos administrativos en el plano de control de la nube. Esto facilita que los atacantes escalen privilegios en dichos entornos.

> *«En los entornos de AWS donde se despliega Aviatrix Controller, la escalada de privilegios está habilitada de manera predeterminada, lo que convierte a esta vulnerabilidad en un riesgo de alto impacto»,* explicaron los investigadores de Wiz: Gal Nagli, Merav Bar, Gili Tikochinski y Shaked Tanchuma.

Los ataques activos que aprovechan la vulnerabilidad CVE-2024-50603 se están utilizando para comprometer instancias en la nube, desplegar el software de minería de criptomonedas XMRig y configurar el marco de comando y control (C2) Sliver, lo que probablemente les

permite mantener acceso y realizar ataques adicionales.

> *«Aunque hasta ahora no hemos observado pruebas concretas de movimiento lateral en la nube, creemos que es probable que los atacantes estén utilizando esta vulnerabilidad para identificar permisos en los entornos afectados y, posteriormente, robar datos de las víctimas»,* señalaron los investigadores de Wiz.

Ante la explotación activa de este fallo, se recomienda a los usuarios instalar las actualizaciones correspondientes lo antes posible y restringir el acceso público al Aviatrix Controller.