Check Point está alertando sobre una vulnerabilidad de día cero en sus productos de gateway de seguridad de red que ha sido explotada por actores maliciosos.

Identificada como CVE-2024-24919, la vulnerabilidad afecta a CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways y Quantum Spark appliances.

> *«La vulnerabilidad podría permitir a un atacante leer cierta información en los gateways conectados a Internet con VPN de acceso remoto o acceso móvil habilitado,»* explicó Check Point.

Las correcciones están disponibles en las siguientes versiones:

- Quantum Security Gateway y CloudGuard Network Security Versions: R81.20, R81.10, R81, R80.40
- Quantum Maestro y Quantum Scalable Chassis: R81.20, R81.10, R80.40, R80.30SP, R80.20SP
- Quantum Spark Gateways Version: R81.10.x, R80.20.x, R77.20.x

Este desarrollo se produce días después de que la compañía de ciberseguridad israelí advirtiera sobre ataques dirigidos a sus dispositivos VPN para infiltrarse en redes empresariales.

> *«Para el 24 de mayo de 2024, identificamos un pequeño número de intentos de inicio de sesión utilizando cuentas locales de VPN antiguas que dependen de un método de autenticación solo por contraseña no recomendado,»* señaló a principios de esta semana.

Esto ahora se ha rastreado hasta una nueva vulnerabilidad de día cero de alta gravedad

descubierta en Security Gateways con IPSec VPN, Remote Access VPN y el software Mobile Access blade.

Check Point no detalló la naturaleza de los ataques, pero indicó en una FAQ que los intentos de explotación observados hasta ahora se enfocan en *«el acceso remoto en cuentas locales antiguas con autenticación no recomendada solo por contraseña un pequeño número de clientes.»*

El ataque a dispositivos VPN representa solo la última serie de ataques dirigidos a aplicaciones de perímetro de red, con ataques similares que afectan a dispositivos de Barracuda Networks, Cisco, Fortinet, Ivanti, Palo Alto Networks y VMware en los últimos años.

> *«Los atacantes están motivados para acceder a organizaciones a través de configuraciones de acceso remoto para intentar descubrir activos y usuarios empresariales relevantes, buscando vulnerabilidades para obtener persistencia en activos empresariales clave,»* explicó Check Point.