BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-13
Fecha de publicación: 30/05/2024
Tema: Vulnerabilidad crítica en VPN Check Point
Traffic Light Protocol (TLP): White

Producto(s) afectado:

Check Point Security Gateways, con acceso remoto VPN o Mobile Access Software Blades habilitado.

Descripción:

Check Point acaba de publicar un parche de seguridad para una vulnerabilidad zero-day en el módulo de VPN que ha sido explotada por los atacantes para ganar acceso remoto a los firewalls y así, intentar comprometer las redes internas.

Esta vulnerabilidad, denominada como CVE-2024-24919, cuenta con una puntuación de 8.6 de severidad, pues permite a los atacantes explotar esta vulnerabilidad de forma remota.

Es importante mencionar que esta vulnerabilidad ya tiene un parche, que soluciona por completo este fallo en el dispositivo, por esto, se recomienda encarecidamente la aplicación del parche lo más pronto posible a todos los usuarios.

Además, el fabricante ha mencionado que desde el día lunes 27 de mayo, se ha visto un incremento considerable en los ataques a sus productos, al poco tiempo, descubrieron que estos ataques son a raíz de la vulnerabilidad antes mencionada.

Impacto

Un actor malintencionado que pueda alcanzar remotamente los aplicativos anteriormente mencionados, podría explotar esta falla, así ganando acceso en el dispositivo, que posteriormente utilizaría para extender su ataque por toda la red corporativa.

Solución

Aplicar el parche oficial publicado por Check Point

Información adicional:

- https://www.bleepingcomputer.com/news/security/check-point-releases-emergency-fix-for-vpn-zero-day-exploited-in-attacks/
- https://nvd.nist.gov/vuln/detail/CVE-2024-24919
- https://thehackernews.com/2024/05/check-point-warns-of-zero-day-attacks.html

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com