Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ALERTA DE CHECK POINT SOBRE ATAQUES ZERO-DAY EN SUS PRODUCTOS VPN

29 / 05 / 2024

CONTENIDO

INTRODUCCIÓN

En una reciente advertencia, Check Point ha revelado la existencia de una grave vulnerabilidad de día cero en varios de sus productos de gateway de seguridad de red, que ya ha sido explotada activamente por ciberdelincuentes. Identificada como CVE-2024-24919, esta vulnerabilidad afecta a productos clave como CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways y Quantum Spark appliances. La explotación de esta falla permite a los atacantes acceder a información sensible en gateways conectados a Internet con acceso remoto VPN o móvil habilitado, lo que subraya la necesidad urgente de aplicar las actualizaciones y medidas de seguridad recomendadas por Check Point.

ALERTA DE CHECK POINT SOBRE ATAQUES ZERO-DAY EN SUS PRODUCTOS VPN

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_05_29_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	29/05/2024
Es día cero (0 day):	SÍ

En una advertencia reciente, Check Point ha informado sobre una vulnerabilidad de día cero en sus productos de gateway de seguridad de red, que ya ha sido explotada por actores malintencionados. Este problema, identificado como CVE-2024-24919, afecta a varios productos clave, incluyendo CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways y Quantum Spark appliances.

Según Check Point, esta vulnerabilidad permite a un atacante leer cierta información en gateways conectados a Internet que tienen habilitado el acceso remoto VPN o el acceso móvil. Este tipo de acceso podría potencialmente exponer información sensible y comprometer la seguridad de las redes empresariales.

Avisos de Check Point

Divulgación de información de VPN de Check Point (CVE-2024-24919)

Vulnerabilidad | **Protección**

Referencia del punto de control:	CPAI-2024-0353
Fecha de publicación:	28 mayo 2024
Severidad:	Alto
Última actualización:	miércoles 29 mayo, 2024
Fuente:	
Referencia de la industria:	CVE-2024-24919
Protección proporcionada por:	**Puerta de enlace de seguridad** R81, R80, R77, R75
¿Quién es vulnerable?	Check Point Quantum Gateway y CloudGuard Network versiones R81.20, R81.10, R81, R80.40. Versiones de Check Point Spark R81.10, R80.20.
Descripción de la vulnerabilidad	Existe una vulnerabilidad de divulgación de información en Check Point VPN. La explotación exitosa de esta vulnerabilidad permitiría a un atacante remoto obtener información confidencial.

Productos y Versiones Afectadas

Las versiones afectadas por esta vulnerabilidad incluyen:

- Quantum Security Gateway y CloudGuard Network Security:** 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:** R81.10.x, R80.20.x, R77.20.x

Check Point ha lanzado hotfixes para estas versiones afectadas, instando a los usuarios a actualizar sus sistemas lo antes posible para mitigar el riesgo.

Contexto del Ataque

La advertencia de Check Point surge días después de que la empresa israelí de ciberseguridad notificara sobre ataques dirigidos a sus dispositivos VPN con el fin de infiltrarse en redes empresariales. Hasta el 24 de mayo de 2024, se identificaron intentos de inicio de sesión utilizando cuentas VPN locales antiguas que dependían de métodos de autenticación únicamente basados en contraseñas, los cuales no son recomendados.

Naturaleza de los Ataques

Aunque Check Point no ha proporcionado detalles específicos sobre la naturaleza de los ataques, mencionó en una FAQ que los intentos de explotación observados hasta ahora se centran en "el acceso remoto en cuentas locales antiguas con autenticación únicamente basada en contraseñas" en un "pequeño número de clientes."

Ataques Perimetrales Recientes

Este ataque a dispositivos VPN es el más reciente de una serie de ataques que han afectado a aplicaciones de perímetro de red, con incidentes similares impactando dispositivos de empresas como Barracuda Networks, Cisco, Fortinet, Ivanti, Palo Alto Networks y VMware en años recientes. Los atacantes están motivados por obtener acceso a organizaciones a través de configuraciones de acceso remoto, buscando descubrir activos empresariales relevantes y usuarios, y encontrar vulnerabilidades para mantener la persistencia en activos clave de la empresa.

Recomendaciones

Dada la gravedad de esta vulnerabilidad, se recomienda a todas las organizaciones que utilicen los productos afectados que apliquen las actualizaciones disponibles de inmediato y revisen sus configuraciones de seguridad, especialmente aquellas que utilicen métodos de autenticación basados únicamente en contraseñas.

NOTICIA COMPLETA

https://devel.group/blog/alerta-de-check-point-sobre-ataques-zero-day-en-sus-productos-vpn/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente