Nro. Alerta:	AL-2025-013	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	07-abr-2025	Brecha de Seguridad en CHECK POINT	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Información
Nivel de riesgo: Alta

II. ALERTA

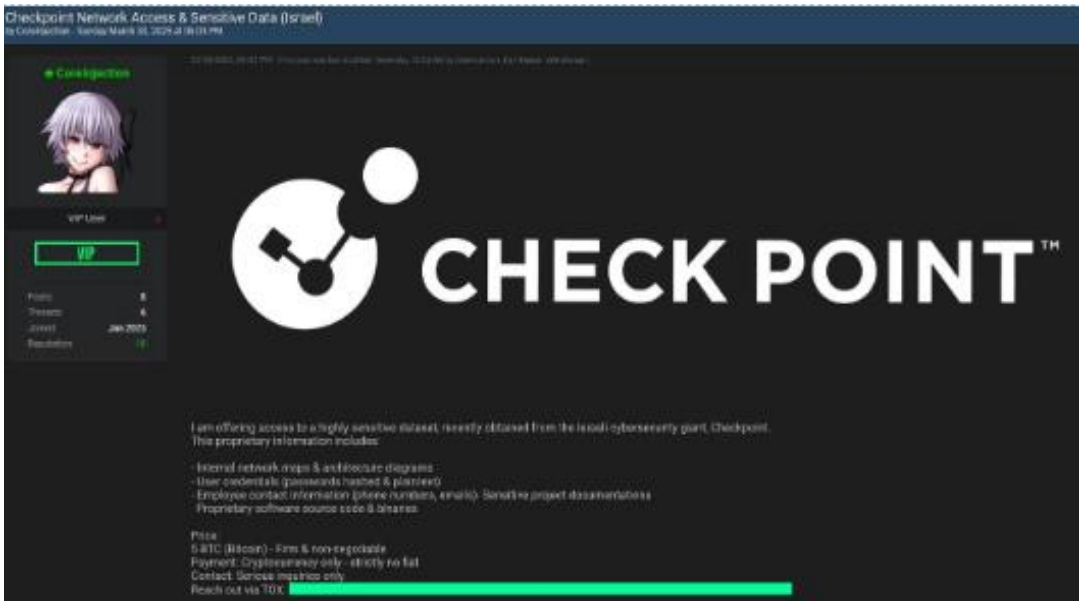

Figura 1.- CHECK POINT- figura referencial

El grupo CoreInjection afirmó haber obtenido datos "altamente sensibles" de la compañía, incluyendo mapas internos de la red, diagramas arquitectónicos, credenciales de usuarios y código fuente propietario de Check Point Software Technologies.

III. INTRODUCCIÓN

Check Point Software Technologies, empresa líder en soluciones de ciberseguridad, sufre una brecha de seguridad y es que CoreInjection ofreció vender información confidencial de clientes en un foro de la dark web, entre la información que los hackers ofrecen incluye mapas de red interna y diagramas de arquitectura, credenciales de usuario en texto y hashed, datos de contacto de los empleados (emails, números de teléfonos), documentación sensible de proyectos, Acceso a nivel de administrador de dashboard (incluyendo más de 121.000 registros de cuenta con casi 19.000 clientes de pagos).

A pesar de las aclaraciones de Check Point, que afirman que el incidente afectó solo a una cuenta de acceso limitado, CoreInjection sostiene que más de 18,000 usuarios fueron comprometidos, lo que pone de manifiesto vulnerabilidades significativas en las prácticas de seguridad.

Los hackers ofrecieron estos datos a la venta en un foro de la Dark Web por 5 bitcoins aproximadamente $410,000, y subieron como evidencia algunas de las capturas de pantalla de los paneles de acceso:

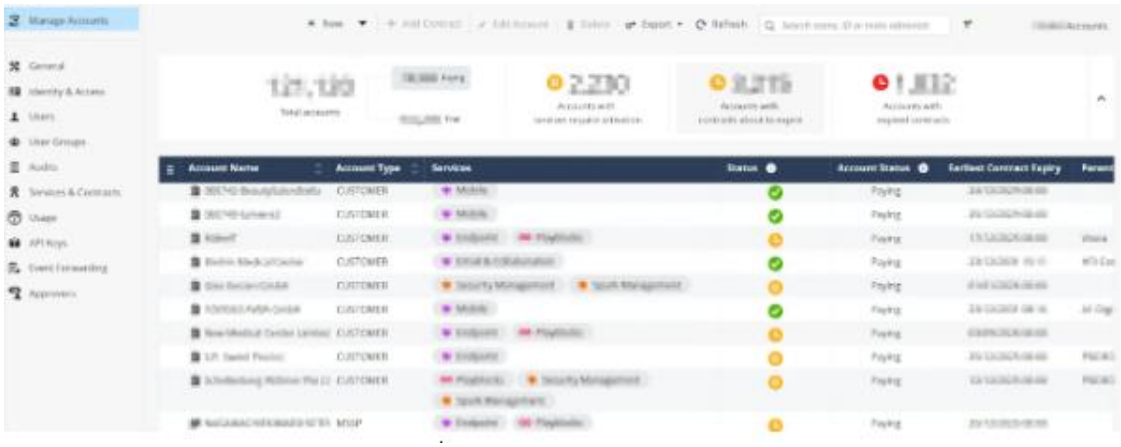

Figura 2.- Pantalla de panel 1

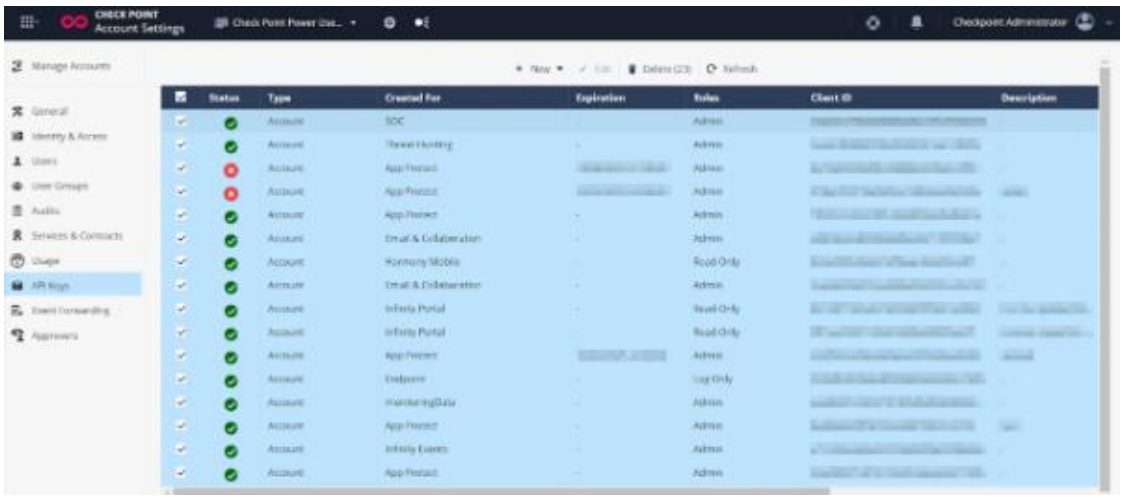

Figura 3.- Pantalla de panel 2

Por su parte la respuesta de Check Point fue:

- La filtración de datos se originó a partir de un incidente antiguo y conocido ocurrido en diciembre de 2024.

- El acceso no autorizado se debió a credenciales comprometidas de una cuenta del portal con acceso limitado.
- La exposición se limitó a unos pocos nombres de cuentas, nombres de productos y algunos datos de contacto de empleados.
- No se vieron afectados los sistemas de clientes, entornos de producción ni arquitecturas de seguridad.
- Las afirmaciones del hacker fueron exageradas y engañosas.

IV. VECTOR DE ATAQUE

Investigadores siguen cuestionando que el método de intrusión sigue siendo desconocido; mencionan credenciales comprometidas, pero no explican cómo (phishing, reuse, etc.), lo cual es preocupante para una empresa de ciberseguridad.

No obstante, en mayo de 2024, la empresa advirtió sobre hackers atacando dispositivos de VPN de Acceso Remoto de Check Point con autenticación insegura basada únicamente en contraseñas. Por lo que se encontró una grave vulnerabilidad denominada CVE-2024-24919, la cual permitía a los hackers leer información confidencial en las Check Point Security Gateways, incluyendo hashes de contraseñas de cuentas locales.

Esta vulnerabilidad recibió una puntuación de 8.6 (alta severidad) en CVSS v3 y fue rápidamente añadida al catálogo de vulnerabilidades explotadas conocidas (KEV) de la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA) de EEUU.

Aunque Check Point asegura que el incidente está contenido y que “no representa ningún riesgo para sus clientes”, los expertos en seguridad siguen cuestionando:

- Cómo obtuvieron acceso inicial los atacantes.
- El verdadero alcance de los datos comprometidos.
- Y por qué no hubo divulgación pública en diciembre de 2024, cuando supuestamente ocurrió la brecha.

V. IMPACTO

La brecha de seguridad expuso vulnerabilidades críticas dentro de la infraestructura de Check Point, poniendo en riesgo la integridad y confidencialidad de los datos. Aunque la empresa ha minimizado el alcance, el impacto potencial podría ser considerable debido a lo siguiente:

1. **Riesgo de robo de datos sensibles:** La filtración de credenciales de acceso podría permitir a los atacantes acceder a información confidencial tanto de clientes como de empleados, lo que podría ser utilizado para futuras campañas de phishing o extorsión.

2. **Aumento de ataques dirigidos:** El acceso a credenciales comprometidas abre la puerta a posibles ataques de repetición, donde los atacantes intentan explotar las credenciales filtradas en otros sistemas o plataformas, aumentando el alcance de la violación de seguridad.

3. **Daño a la reputación:** La filtración de datos y la posible exposición de información confidencial pueden afectar seriamente la reputación de Check Point, ya que clientes, socios y reguladores pueden perder confianza en su capacidad para proteger datos sensibles.

4. **Posibles sanciones regulatorias:** En función del tipo de datos filtrados y las leyes de protección de datos aplicables, Check Point podría enfrentar sanciones o multas de organismos reguladores, especialmente si no se tomaron medidas adecuadas para proteger la información confidencial.

VI. RECOMENDACIONES:

Para mitigar el riesgo de futuros incidentes y protegerse contra amenazas similares, se recomienda:

- Implementar Autenticación Multifactor (MFA) en todas las cuentas, especialmente en aquellas con privilegios administrativos o acceso a datos sensibles.
- Auditar y rotar regularmente las credenciales de cuentas sensibles, asegurando que las contraseñas sean fuertes y únicas.
- Limitar privilegios administrativos mediante el principio de mínimo privilegio, para que los usuarios solo tengan acceso a la información estrictamente necesaria.
- Monitorear la red y los sistemas para detectar accesos inusuales o intentos de explotación de credenciales comprometidas.
- Actualizar y aplicar parches de seguridad de manera regular para mitigar vulnerabilidades conocidas que puedan ser explotadas por atacantes.
- Realizar análisis forenses de seguridad para determinar el alcance real de la brecha y prevenir futuras intrusiones.
- Concienciar a los empleados sobre riesgos de phishing y cómo gestionar de manera segura las credenciales de acceso.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

https://www.cybersecuritydive.com/news/check-point-software-security-incident/744198/

https://support.checkpoint.com/results/sk/sk183307

https://www.theregister.com/2025/03/31/check_point_confirms_breach/

https://www.securityweek.com/check-point-responds-to-hacking-claims/

https://cybersecuritynews.com/check-point-acknowledges-data-breach/

https://socradar.io/alleged-check-point-breach-what-happened-and-what-you-need-to-know/

https://cybernews.com/security/check-point-data-for-sale-firm-says-no-risk/