Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CVE-2025-3831: LOGS DE HARMONY SASE DE CHECK POINT EXPUESTOS VÍA SERVIDOR SFTP COMPARTIDO

12/ 08 / 2025

CONTENIDO

INTRODUCCIÓN 3

RESUMEN 5

NOTICIA COMPLETA 6

CONTACTOS DE SOPORTE 7

INTRODUCCIÓN

La seguridad de la información en entornos corporativos no solo depende de la protección de los sistemas en producción, sino también de los mecanismos de soporte y diagnóstico. Un error en estos procesos puede exponer datos sensibles sin que el cliente lo perciba. Tal es el caso de la vulnerabilidad recientemente identificada en el agente Harmony SASE de Check Point, registrada como CVE-2025-3831, que puso en riesgo la confidencialidad de archivos de diagnóstico subidos a un servidor SFTP.

Este fallo, clasificado con severidad alta, permitió que los logs enviados por clientes durante tareas de soporte técnico fueran accesibles para terceros no autorizados debido a una mala configuración de permisos. La exposición potencial de tokens de autenticación temporales y otra información sensible ha encendido las alarmas en la comunidad de ciberseguridad, resaltando la importancia de aplicar el principio de menor privilegio incluso en canales que tradicionalmente se consideran seguros.

GUNRA RANSOMWARE: NUEVA VARIANTE PARA LINUX REFUERZA CAPACIDADES DE CIFRADO MASIVO Y PERSONALIZACIÓN

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

ID de alerta:	DSOC-CERT_2025_08_12_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	12/08/2025
Es día cero (0 day):	No

RESUMEN

Check Point confirmó que los archivos de logs que el agente Harmony SASE subía a un servidor SFTP durante procesos de *troubleshooting* pudieron haber sido accesibles por terceros no autorizados debido al uso de una clave SFTP compartida con permisos de lectura/listado, en lugar de permisos liChemitados sólo a escritura.
Entre los datos potencialmente expuestos se encuentran tokens de autenticación temporales contenidos en esos ficheros de diagnóstico.
El problema aparece en el registro público de asesorías y bases de datos de vulnerabilidades bajo el identificador CVE-2025-3831.

¿Qué pasó?

- El agente de Harmony SASE incluía en su flujo de subida de logs una clave SFTP embebida/compartida usada para enviar archivos de diagnóstico a un servidor de soporte.
- Esa clave tenía permisos para leer y listar el contenido del servidor SFTP, no sólo para subir (*write-only*).
- Por tanto, cualquiera con acceso a la clave podía listar y descargar logs de otros clientes.
- Los logs de diagnóstico suelen contener información sensible, rutas, errores y, en algunos casos, tokens temporales o fragmentos de sesiones, lo que supone un riesgo significativo de exposición de datos.

Línea de tiempo y desenlace

- 22 de marzo de 2025: Check Point detectó la falla en el mecanismo de subida de logs del agente Harmony SASE y procedió a corregirla de inmediato.
- Se restringieron los permisos de la clave SFTP compartida para que solo permitiera operaciones de escritura (*write-only*), eliminando la capacidad de leer o listar archivos.
- La compañía comunicó públicamente el incidente y confirmó que **no se requiere ninguna acción por parte de los clientes** en este momento, dado que la vulnerabilidad ya fue mitigada.

Impacto y severidad

- La exposición se clasifica como alta, ya que permite acceso a información sensible (CWE-200: Exposure of Sensitive Information).
- Herramientas de seguimiento de CVE y agregadores califican el impacto como significativo para los clientes que utilizaron el mecanismo vulnerable de subida de logs.

Solución aplicada por el proveedor

- **Mitigación inmediata:** Check Point limitó los permisos del par de claves en el servidor SFTP a *write-only*.
- **Comunicación:** Publicación de un aviso oficial en su portal de seguridad, confirmando que la vulnerabilidad fue cerrada y que no se requiere acción por parte del cliente.

Buenas prácticas y recomendaciones (como expertos en ciberseguridad)

Aunque Check Point mitigó el problema, las organizaciones deben reforzar sus procesos internos para prevenir incidentes similares:

1. **Verificar con el proveedor**
    - Confirmar la versión del agente y revisar boletines de seguridad relacionados con CVE-2025-3831.
2. **Revisar logs y tokens emitidos**
    - Auditar tokens o credenciales temporales que pudieron haberse incluido en logs. Rotarlos si es necesario.
3. **Segregar canales de soporte**
    - Usar credenciales únicas por cliente o mecanismos de subida con permisos estrictos.
4. **Aplicar el principio de menor privilegio**
    - Limitar accesos de credenciales de diagnóstico únicamente a la función que necesitan cumplir.
5. **Cifrado y DLP en repositorios de logs**
    - Implementar controles para detectar y proteger datos sensibles antes de que se almacenen.
6. **Rotación y monitoreo de credenciales**
    - Rotar claves SFTP y monitorear accesos inusuales o intentos de listado masivo de archivos.
7. **Pruebas de seguridad periódicas**
    - Incluir auditorías y *pentests* sobre los canales de telemetría y diagnóstico.
8. **Plan de respuesta ante incidentes**
    - Tener definido un protocolo claro para contención, análisis forense y notificación si se detecta acceso no autorizado.

llamada a la acción

CVE-2025-3831 es un recordatorio de que los canales de soporte y diagnóstico pueden convertirse en un punto débil si no se aplican principios de mínimo privilegio y control de accesos. Check Point ya mitigó la vulnerabilidad, pero es recomendable que las organizaciones verifiquen sus configuraciones, auditen sus logs y fortalezcan sus procedimientos para manejar credenciales y datos de diagnóstico de manera segura.

NOTICIA COMPLETA

https://devel.group/blog/cve-2025-3831-logs-de-harmony-sase-de-check-point-expuestos-via-servidor-sftp-compartido/

CONTACTOS DE SOPORTE

Correo electrónico: teamcti@devel.group

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://devel.group/