BOLETÍN DE SEGURIDAD

Campaña avanzada de GT13 expone entornos de administración Check Point – 25 Noviembre 2026

NOVIEMBRE 2026

El material incluido en este documento es propiedad exclusiva de SOFTSECURITY SAS. Este documento no puede ser divulgado de cualquier manera o a cualquier persona a excepción del destinatario y los empleados o representantes de la firma a quien va dirigido, quienes son los directamente responsables de la evaluación de su contenido. Este documento no puede ser utilizado en cualquier forma diferente al propósito con el que fue distribuido. Se prohíbe terminantemente cualquier uso, reproducción o transmisión no autorizada.

INTRODUCCIÓN

En un mundo cada vez más conectado, la ciberseguridad no es solo responsabilidad del área de TI: es un compromiso de todos. Este boletín tiene como objetivo mantenerte informado sobre las amenazas más recientes, las buenas prácticas de seguridad digital y las acciones clave que puedes tomar para proteger tanto tu información personal como los activos de las organizaciones.

En el siguiente informe se encontrará información sobre amenazas actuales, recomendaciones e indicadores de compromiso.

¿Qué se conoce sobre la campaña avanzada de GT13 que expone entornos de administración Check Point?

GreyNoise ha documentado una campaña, a la que denomina GT13, en la que un atacante comprometió 24 servidores de gestión de Check Point (Security Management Server, SMS) pertenecientes a, al menos, 22 organizaciones de 17 países. El atacante abusó de CVE-2026-16232, un bypass de autenticación de SmartConsole con puntuación CVSS v4.0 de 9,3, para enviar tareas de administración a los servidores y, en el caso mejor documentado, extraer la configuración, la base de reglas, los usuarios y la autoridad certificadora (CA) interna.

Un servidor de gestión es el punto desde el que se administran las políticas, los certificados y las VPN de los firewalls gestionados, por lo que su compromiso permite llegar a los dispositivos que protegen la red. GreyNoise documenta actividad entre el 17 de octubre y el 2 de noviembre de 2026, aunque el servidor puente que usó el atacante fue comprometido desde el 2 de octubre. No ha podido determinar cuándo ni cómo accedió el atacante a los servidores de gestión y considera que la campaña podría seguir activa, porque conserva acceso persistente. Al momento de publicarse el análisis, Check Point no se había pronunciado públicamente sobre la campaña.

Datos clave

- **Actor:** GT13 es la denominación de GreyNoise. No se atribuye a un grupo conocido y no se conoce su país de origen ni su motivación. Existen indicios no concluyentes (franjas horarias UTC+7/UTC+8 y un dominio con registrante en Hai Phong, Vietnam) a los que el propio laboratorio da poco peso. GreyNoise plantea, como hipótesis, el uso de un sistema ofensivo asistido por IA.
- **Víctimas:** 24 servidores de gestión en al menos 22 organizaciones de 17 países: Reino Unido, Irlanda, Francia, Países Bajos, Grecia, Alemania, Austria, Bulgaria, Polonia, India, Tailandia, Vietnam, Corea del Sur, Hong Kong, China, Australia y Estados Unidos.
- **Sectores:** servicios financieros, energía, administración pública, transporte, minería, ingeniería y fabricación, sin un patrón claro.
- **Víctima más afectada («Víctima A»):** organización con dos SMS en la misma red. Sufrió la mayor parte de la intrusión, con 227 inicios de sesión en el primer SMS, y el segundo SMS fue alcanzado mediante un túnel.
- **Relación con otras campañas:** GreyNoise considera que GT13 no está relacionada con la campaña PHP2Shell contra gateways de Check Point, aunque sus fechas se solapan.

Análisis de las vulnerabilidades

1. CVE-2026-16232: bypass de autenticación en Check Point SmartConsole (CWE-287)

Afecta a Security Management Server y Multi-Domain Security Management. El servicio FWM/CPMI (puerto TCP 18190) acepta como identidad el DN de SIC que envía el cliente, en lugar del que figura en el certificado. El atacante lee el DN del servidor, obtiene un token de aplicación, solicita un ticket SSO con permisos system_admin y lo canjea por SOAP en el servicio CPM (puerto TCP 19009). Tiene CVSS v4.0 de 9,3 (Check Point como CNA) y CVSS v3.1 de 9,8 (NVD), se explota activamente y fue incluida en el catálogo KEV de CISA el 22 de julio de 2026.

Versiones afectadas y corregidas

- Afectadas: R81.10, R81.20, R82 y R82.10, y anteriores.
- Corregidas con el Jumbo Hotfix del 22 de julio de 2026: R82.10 desde Take 36, R82 desde Take 118 y R81.20 desde Take 158. Smart-1 Cloud ya estaba protegido.
- Sin corrección publicada, según Rapid7: R81.10, R81 y las ramas R80 y R77.30.

La configuración de Trusted Clients que no restringe los clientes GUI venía por defecto en las pruebas de Rapid7. Las explotaciones dejan en el registro de auditoría la línea «Authentication method: application token».

2. CVE-2026-61500: Rejetto HFS 3.0.0 a 3.2.0

El atacante lo usó el 2 de octubre para comprometer un servidor Ubuntu con HFS sin parchear, que empleó como puente (relé). HFS deriva la clave de firma de las cookies de sesión con Math.random(), un generador no criptográfico, y filtra sus salidas en el inicio de sesión. Con unas pocas respuestas se reconstruye el estado del generador, se recupera la clave y se forja una cookie de administrador. Tiene CVSS v3.1 de 9,8 (NVD) y CVSS v4.0 de 9,3 (VulnCheck), y se corrigió en HFS 3.2.1.

GT13 también comprobó CVE-2026-98432 (use-after-free en la pila IPv4 del kernel Linux, CVSS v3.1 de 9,8) en el relé el 2 de noviembre. Contra la Víctima A probó, el 21 de octubre, exploits de CVE-2020-1472 (Zerologon), CVE-2023-4966 (CitrixBleed), CVE-2024-21893 (Ivanti Connect Secure), CVE-2021-26855 y CVE-2021-34473 (Exchange), y CVE-2021-21972 y CVE-2023-34048 (vCenter).

3. Cronología de la intrusión (UTC)

- **2 de octubre:** compromiso del servidor HFS con CVE-2026-61500 y primeras peticiones de administración con cookies falsificadas. El 5 de octubre se añadió un hook en HFS y una clave SSH en /root/.ssh/authorized_keys.
- **19 y 20 de octubre:** intento fallido de descargar el implante ZULT y regreso por SSH para montar el relé manualmente.
- **20 a 26 de octubre:** explotación de CVE-2026-16232. El 21 de octubre copió ficheros de configuración y de la CA del segundo SMS de la Víctima A, descargó su política de seguridad y probó exploits contra controladores de dominio, Citrix, Ivanti, Exchange y vCenter.
- **26 de octubre (02:17):** tarea masiva de certificados a los 24 servidores. Falló en todos, pero las respuestas de error permitieron al atacante identificar a las víctimas.
- **2 de noviembre:** comprobación de CVE-2026-98432 y cambio de reglas nftables en el relé. Es la última actividad registrada (03:19).
- **23 de noviembre:** GreyNoise publica su informe.

4. Herramientas e infraestructura

- **Herramientas de terceros:** Nmap, Chisel (túnel/proxy), Impacket y Paramiko.
- **Scripts propios en Python:** exploit.py (para CVE-2026-16232), comb.py, ssh_comb.py y ssh_spray.py (fuerza bruta y password spraying por SSH y web) y un receptor en el puerto 8001.
- **Implantes:** ZULT (Linux), descargado desde data-zt[.]newpayapp[.]com, y un posible implante en modo usuario, /usr/lib/.libproc.so, registrado en /etc/ld.so.preload (GreyNoise lo presenta como indicador posible, sin confirmar).
- **Infraestructura:** 99 direcciones IP, la mayoría de ExpressVPN (AS206092) y algunas de equipos Check Point ya comprometidos, con más de 1.400 sesiones de red registradas.

5. Impacto

- **Datos exfiltrados de la Víctima A:** /etc/shadow y /etc/passwd, usuarios locales (fwauth.NDB), ficheros de la CA interna, sic_cert.p12 y SIC_DB, listas de administradores, objetos de red, servicios, autenticación y LDAP, y la base de reglas.
- **CA interna comprometida:** permite emitir certificados que la instalación acepta, incluidos los de la comunicación entre gestión y gateways y los de VPN IPsec basadas en certificados. Se identificó un certificado malicioso (pivot.p12) emitido con la CA de la Víctima A.
- **Política de seguridad descargada:** el atacante conoce las reglas del firewall, lo que, según el artículo, equivale a dejarlo sin reglas.
- **Alcance incierto:** no estar en la lista de organizaciones avisadas por GreyNoise no equivale a estar limpio, porque esa lista no se ha publicado.

Recomendaciones

De acuerdo con lo mencionado en el informe de GreyNoise, el aviso de Check Point, el análisis de Ciberseguridad.blog y Brandefense y de parte de Softsecurity se recomienda llevar a cabo las siguientes acciones:

- **Bloqueo IoC's:** Se recomienda bloquear los indicadores de compromiso listados en el presente boletín en las herramientas de seguridad perimetal.
- **Verificación y actualización:** Comprobar que el SMS o Multi-Domain tiene el Jumbo Hotfix de julio de 2026 (R82.10 Take 36, R82 Take 118 o R81.20 Take 158) y listar los hotfix instalados con cpinfo. Si se usa R81.10 o una versión anterior, planificar la migración a una versión corregida, porque no hay parche publicado.
- **Reducción de la exposición:** Restringir Trusted Clients en SmartConsole a las IP o subredes de administración y eliminar cualquier entrada «Any». Cerrar desde Internet los puertos TCP 18190 y 19009 y acceder a la gestión solo por VPN o redes dedicadas.
- **Detección de posible compromiso:** Buscar «application token» en el registro de auditoría desde el 22 de julio y, sobre todo, desde el 2 de octubre; los inicios de sesión con ese método que no correspondan a integraciones conocidas son sospechosos. Revisar desde el 17 de octubre el historial de política y de la CA interna: descargas de política no solicitadas, certificados emitidos fuera de cambios planificados y tareas nocturnas. En modo experto, revisar /etc/ld.so.preload, /usr/lib/.libproc.so, authorized_keys de root y de los usuarios, y buscar pivot.p12.
- **Respuesta ante indicios:** Conservar una imagen del servidor antes de modificarlo, revocar los certificados no reconocidos, restablecer SIC con los gateways, cambiar las contraseñas de los administradores y de las cuentas LDAP almacenadas, y reinstalar desde una versión corregida. Activar el procedimiento de respuesta a incidentes.
- **Sistemas de terceros:** Verificar que los controladores de dominio, Citrix NetScaler, Ivanti Connect Secure, Exchange y vCenter tienen los parches de los CVE citados, y que cualquier instancia de Rejetto HFS esté en la versión 3.2.1 o superior.

Indicadores de compromiso

- **Dominios:**
  - newpayapp[.]com
  - data-zt[.]newpayapp[.]com
  - api-zt[.]newpayapp[.]com
  - 2ev5[.]newpayapp[.]com.
- **Direcciones IP:**
  - 45[.]92[.]229[.]10
  - 45[.]92[.]229[.]9
  - 63[.]135[.]161[.]27
  - 45[.]130[.]83[.]138
  - 45[.]8[.]19[.]209
  - 216[.]73[.]161[.]174
  - 45[.]8[.]19[.]244
  - 216[.]73[.]161[.]233
  - 216[.]73[.]161[.]107
  - 216[.]73[.]160[.]129
- **Archivos y certificados:** /usr/lib/.libproc.so, entradas en /etc/ld.so.preload, pivot.p12, ficheros con prefijo pc_ copiados por scp y claves SSH no reconocidas en /root/.ssh/authorized_keys.
- **Registro de auditoría:** líneas con «Authentication method: application token» que no correspondan a integraciones conocidas.
- **Tráfico y servicios:** conexiones a los puertos TCP 18190 y 19009 desde direcciones no administrativas, y servicios Chisel (9000) y receptor Python (8001) en el relé del atacante.
- **HTTP:** cookie hfs_http falsificada con allow_session_ip_change en true y user-agents tipo Mozilla/5.0 que incluyen la palabra «research».

Referencias

Ramiro, R. (2026, noviembre 24). Un atacante robó datos de 24 servidores de gestión de Check Point. Ciberseguridad.blog. Recuperado de https://ciberseguridad.blog/check-point-gt13-servidores-gestion/

Miller, S. (2026, noviembre 23). 99 IPs but a C2 ain't one. GreyNoise. Recuperado de https://www.greynoise.io/blog/check-point-security-management-servers-intrusion-campaign

Check Point. (2026, julio 22). Security advisory: Action required, active exploitation of Check Point SmartConsole authentication bypass (CVE-2026-16232). Recuperado de https://blog.checkpoint.com/security/security-advisory-action-required-active-exploitation-of-check-point-smartconsole-authentication-bypass-cve-2026-16232

Rapid7. (2026, julio 28). Check Point SmartConsole authentication bypass: Technical analysis (CVE-2026-16232). Recuperado de https://www.rapid7.com/blog/post/ra-check-point-smartconsole-authentication-bypass-technical-analysis-cve-2026-16232/

Brandefense Research Team. (2026, noviembre 24). GT13 reaches Check Point management servers at 22 organizations. Brandefense. Recuperado de https://brandefense.io/security-news/gt13-check-point-management-intrusions/