GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °3026

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	3	0	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

CVE-2026-16232 – CHECK POINT SMARTCONSOLE (BYPASS DE AUTENTICACIÓN Y ACCESO ADMINISTRATIVO REMOTO)

Se ha divulgado y confirmado la explotación activa en entornos reales de una vulnerabilidad crítica de omisión de autenticación (Authentication Bypass) que afecta al proceso de inicio de sesión de SmartConsole en las soluciones de gestión de seguridad Security Management Server y Multi-Domain Security Management (MDS) de Check Point.

El fallo, rastreado como CVE-2026-16232, permite a un atacante remoto no autenticado obtener un token de inicio de sesión de la aplicación y autenticarse con privilegios administrativos completos, lo que faculta la modificación arbitraria de políticas de seguridad y configuraciones en toda la arquitectura administrada. La Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (CISA) incorporó de forma urgente este fallo en su catálogo de Vulnerabilidades Explotadas Conocidas (KEV).

Resumen técnico:

- Identificador principal: CVE-2026-16232.
- Severidad: Crítica (Puntaje base de 9.3 por el fabricante / 9.1 bajo el estándar CVSS v3.1).
- Causa raíz: Fallo de límite de confianza e inadecuada autenticación (Improper Authentication / CWE-287) dentro de la ruta de autenticación de aplicaciones de la clase LoginSvcImpl.
- Mecanismo de falla: El componente afectado acepta un nombre distinguido (Distinguished Name - DN) del mecanismo de comunicación interna segura (SIC) proporcionado directamente por el atacante en lugar de validarlo y vincularlo contra el DN del certificado del par autenticado devuelto por getCertificateDnName(). Un atacante remoto sin credenciales lee el DN SIC del servidor durante la fase inicial no autenticada en el servicio FWM/CPMI (puerto TCP 18190), reitera dicho DN en una solicitud de enlace de certificado falsificada, obtiene un token de aplicación DLE y posteriormente solicita un ticket de inicio de sesión único (SSO) de SmartConsole para ingresar con privilegios de system_admin a través de la API SOAP de CPM/DLE (puerto TCP 19009).
- Estado de explotación: Explotación activa confirmada en entorno real como vulnerabilidad Zero-Day, incluida en el catálogo KEV de CISA. Se cuenta con análisis técnicos detallados de causa raíz y código de prueba de concepto (PoC) público plenamente funcional.
- Versiones afectadas: Servidores de gestión Check Point Security Management y Multi-Domain Management en versiones R77.30, R80, R80.10, R80.20, R80.30, R81, R81.10, R81.20 (anteriores a Jumbo Hotfix Take 158), R82 (anteriores a Take 118) y R82.10 (anteriores a Take 36).

Impacto potencial:

- Toma de control administrativo absoluto de la infraestructura de gestión: Un atacante no autenticado obtiene acceso completo como administrador de sistema (system_admin), lo que le permite alterar las configuraciones centrales de la plataforma y modificar usuarios administrativos.
- Modificación arbitraria de políticas de seguridad y VPN en gateways administrados: Al comprometer el servidor de gestión central, el atacante puede desplegar reglas permisivas, desactivar inspecciones de seguridad o alterar túneles VPN en todas las pasarelas (Security Gateways) bajo su control.
- Evasión de detección y desactivación de registros de auditoría: La toma de acceso privilegiado faculta al actor de amenazas para deshabilitar el monitoreo en tiempo real, alterar los registros de auditoría o manipular eventos de seguridad para ocultar sus actividades en la red.
- Movimiento lateral e interceptación de tráfico corporativo: El control del servidor perimetral de administración actúa como punto de apoyo estratégico para extraer secretos corporativos, exfiltrar configuraciones topológicas y pivotar hacia otros segmentos de la red interna.

Recomendaciones de mitigación:

1. Aplicación inmediata del Jumbo Hotfix oficial de Check Point: Desplegar con carácter de emergencia los parches oficiales publicados por el fabricante según la versión instalada (R81.20 Jumbo Hotfix Take 158, R82 Take 118 y R82.10 Take 36 o superiores).
2. Restricción estricta de clientes confiables (Trusted Clients): Modificar la configuración de clientes GUI de SmartConsole para permitir únicamente direcciones IP o subredes explícitamente autorizadas, eliminando cualquier regla predeterminada que admita acceso desde cualquier origen (Any).
3. Endurecimiento perimetral y aislamiento de puertos de gestión: Bloquear el acceso directo desde Internet a los puertos de gestión del servidor (TCP 18190 y TCP 19009) mediante reglas de firewall estrictas, restringiendo su exposición a redes internas o vías seguras de acceso remoto (VPN/ZTNA).
4. Cacería de amenazas e inspección de indicadores de compromiso (IoCs): Auditar los registros de auditoría del servidor de gestión en busca de eventos sospechosos como "Authentication method: application token" o registros de conexión procedentes de las direcciones IP maliciosas reportadas (151.241.99.207, 151.241.99.233, 158.62.198.182, 192.142.10.99, 139.28.37.250, 194.213.18.137).

Prioridad: Crítica.

Ampliar información:

- https://www.rapid7.com/blog/post/ra-check-point-smartconsole-authentication-bypass-technical-analysis-cve-2026-16232/
- https://thehackernews.com/2026/07/rapid7-releases-poc-for-exploited-check.html
- https://www.greenbone.net/en/blog/check-point-smartconsole-vulnerability/
- https://csirt.telconet.net/comunicacion/boletines-servicios/bypass-de-autenticacion-en-check-point-smartconsole-explotado-activamente/
- https://www.rapid7.com/blog/post/etr-cve-2026-16232-critical-check-point-smartconsole-authentication-bypass-exploited-in-the-wild/
- https://securityaffairs.com/195848/hacking/check-point-patches-actively-exploited-smartconsole-authentication-bypass-flaw.html

CVE-2026-59309 Y CVE-2026-59310 – VMWARE VCENTER (BYPASS DE AUTENTICACIÓN Y EJECUCIÓN REMOTA DE CÓDIGO)

Broadcom publicó actualizaciones de emergencia para corregir las vulnerabilidades críticas **CVE-2026-59309** y **CVE-2026-59310** en **VMware vCenter Server**, componente central de administración de **vSphere** y **VMware Cloud Foundation**. Estos fallos permiten a atacantes remotos no autenticados evadir controles de acceso o ejecutar código arbitrario con privilegios de sistema. Su explotación compromete el plano de gestión de la infraestructura virtualizada, exponiendo los hosts **ESXi**, las máquinas virtuales, los almacenes de datos y las configuraciones de red corporativas.

Resumen técnico:

- Identificadores principales: CVE-2026-59309 y CVE-2026-59310.
- Severidad: Crítica (Puntaje base CVSS v3.1 de 9.8 para ambas vulnerabilidades).
- Causa raíz: Fallo de omisión de autenticación en VMware Directory Service (vmdird) [CVE-2026-59309] y recorrido de directorios (Directory Traversal) en el servicio vCenter Syslog Server [CVE-2026-59310].
- Mecanismo de falla: En CVE-2026-59309, un atacante remoto con acceso a la red de gestión puede interactuar con el servicio de directorio sin credenciales previas para evadir la autenticación y obtener acceso no autorizado a la plataforma. En CVE-2026-59310, la manipulación de rutas en el servidor Syslog permite escribir archivos no autorizados y lograr la ejecución remota de código (RCE) de forma no autenticada.
- Estado de explotación: Sin evidencias de explotación activa en el momento de la divulgación; no obstante, Broadcom señala que no existen mitigaciones temporales (workarounds) y recomienda tratar la actualización como un cambio de emergencia.
- Versiones afectadas: VMware vCenter Server 8.0 (anteriores a 8.0 U3k), VMware Cloud Foundation / vSphere Foundation 9.0.x (anteriores a 9.0.2.0100), 9.1.x (anteriores a 9.1.0.0300), VMware Cloud Foundation 5.x (vía parche asincrónico) y soluciones VMware Telco Cloud (versiones 3.0, 4.x, 5.0.x y 5.1.x).

Impacto potencial:

- Compromiso total del plano de gestión de virtualización: La explotación exitosa de la omisión de autenticación permite a actores maliciosos acceder sin autorización a la consola vCenter, obteniendo control administrativo sobre la infraestructura virtualizada.
- Ejecución remota de código (RCE) con privilegios de sistema: El fallo de recorrido de directorios en el servicio Syslog faculta a atacantes remotos a ejecutar comandos arbitrarios directamente en el servidor vCenter (VCSA), tomando control del sistema operativo subyacente.
- Movimiento lateral e interrupción de hosts ESXi y VMs: Al controlar la consola central, un atacante puede manipular configuraciones de hipervisores, acceder a las consolas interactivas de las máquinas virtuales, alterar redes virtuales o apagar servicios críticos.
- Persistencia en el dominio SSO y alteración de auditorías: La toma de control del servicio de directorio faculta a los atacantes para crear usuarios fraudulentos en el dominio Single Sign-On (SSO), alterar permisos globales y manipular registros de auditoría para encubrir sus actividades.

Recomendaciones de mitigación:

1. Aplicación urgente de parches de seguridad oficiales: Actualizar de forma inmediata las instancias de vCenter Server a las versiones corregidas por el fabricante: 8.0 U3k, 9.0.2.0100 o 9.1.0.0300 (o desplegar el parche asincrónico correspondiente en entornos Cloud Foundation 5.x).
2. Aislamiento y segmentación estricta del plano de gestión: Restringir el acceso de red hacia las interfaces y puertos de vCenter Server únicamente a subredes de administración dedicadas y equipos bastión (Jump Hosts), bloqueando cualquier conexión proveniente de la red corporativa general o Internet.
3. Refuerzo de controles de acceso e identidad en vSphere: Implementar autenticación multifactor (MFA) en los puntos de entrada remotos a la red de gestión y segmentar estrictamente los privilegios del dominio SSO de vCenter respecto a los directorios corporativos estándar.
4. Auditoría de logs de directorio y monitoreo de eventos: Revisar periódicamente los registros del servicio de directorio (/var/log/vmware/vmdird/) y las tareas administrativas de vCenter en busca de inicios de sesión anómalos, creación no autorizada de roles/usuarios o peticiones inusuales dirigidas al servicio Syslog.

Prioridad: Crítica.

Ampliar información:

- https://www.rapid7.com/blog/post/etr-critical-vmware-vcenter-vulnerabilities-allow-authentication-bypass-and-remote-code-execution-cve-2026-59309-cve-2026-59310/
- https://thehackernews.com/2026/07/three-critical-vmware-flaws-allow-auth.html
- https://www.penligent.ai/hackinglabs/cve-2026-59309/
- https://fieldeffect.com/blog/broadcom-patches-critical-vcenter-vulnerabilities
- https://www.it-connect.tech/vmware-3-critical-flaws-in-vcenter-and-esx-including-a-vm-escape/

CVE-2026-66066 – RUBY ON RAILS ACTIVE STORAGE (LECTURA DE ARCHIVOS Y EJECUCIÓN REMOTA DE CÓDIGO)

Se ha divulgado una vulnerabilidad crítica que afecta al componente Active Storage de Ruby on Rails cuando utiliza la biblioteca libvips para el procesamiento de variantes de imágenes. Identificado como CVE-2026-66066 (apodado por investigadores como KindaRails2Shell), este fallo permite a atacantes remotos no autenticados leer archivos arbitrarios del servidor y escalar a la ejecución remota de código (RCE) mediante la carga de archivos de imagen especialmente diseñados.

Debido a que **Active Storage** con el procesador **vips** se configura por defecto en Docker oficial de **Rails** y en distribuciones **Debian/Ubuntu** desde la versión **7.0**, un gran número de aplicaciones en producción que permiten la carga de imágenes por usuarios no confiables se encuentran expuestas de forma predeterminada.

Resumen técnico:

- Identificador principal: CVE-2026-66066.
- Severidad: Crítica (Puntaje base CVSS v4 de 9.5 / CVSS v3.1 de 9.5).
- Causa raíz: Configuración predeterminada insegura (CWE-1188) e inadecuado manejo de límites de confianza entre Active Storage y el motor libvips.
- Mecanismo de falla: libvips utiliza "cargadores" (loaders) respaldados por bibliotecas de terceros, algunos de los cuales están marcados como "no probados/inseguros" (unfuzzed) para contenido no confiable. Active Storage no deshabilitaba estas operaciones inseguras al procesar variantes (miniaturas, avatares o previsualizaciones). Un atacante remoto sin autenticación puede subir una imagen maliciosa que fuerce la invocación de uno de estos cargadores inseguros, permitiendo la exfiltración de archivos del sistema de archivos donde corre el trabajador de Rails (incluyendo las variables de entorno del proceso y llaves criptográficas).
- Estado de explotación: Divulgada a finales de julio de 2026. Se registran pruebas de concepto (PoC) públicas capaces de reconstruir la cadena de exfiltración de llaves (secret_key_base) para firmar cargas maliciosas y obtener RCE.
- Versiones afectadas: Rails activestorage en versiones < 7.2.3.2, 8.0.0 a 8.0.5.0 y 8.1.0 a 8.1.3.0 (en su configuración por defecto). Las versiones de la rama 6.x (6.0.0 - 6.1.7.10) se ven afectadas únicamente si el procesador vips fue habilitado manualmente.

Impacto potencial:

- Lectura arbitraria de archivos del sistema (Arbitrary File Read): Permite a un atacante no autenticado leer cualquier archivo accesible en el sistema de archivos del servidor por el proceso del trabajador de Rails.
- Fuga masiva de secretos y llaves maestras de la aplicación: Faculta el robo de la variable secret_key_base, la llave maestra (master.key / config/credentials.yml.enc), contraseñas de bases de datos, llaves de almacenamiento en la nube (AWS S3, Azure Blob, GCS) y tokens de API de terceros.
- Escalada a ejecución remota de código (RCE): Mediante la exfiltración de secret_key_base y las llaves maestras, un atacante puede generar cookies de sesión falsificadas, firmar payloads de deserialización o forzar ejecuciones de comandos en el sistema operativo servidor.
- Compromiso lateral de la infraestructura corporativa: El robo de credenciales de servicios externos y bases de datos permite al atacante pivotar hacia otros sistemas interconectados en la nube o en la red interna.

Recomendaciones de mitigación:

1. Actualización inmediata del marco Ruby on Rails: Desplegar de forma prioritaria la actualización del paquete activestorage a las versiones corregidas 7.2.3.2, 8.0.5.1 o 8.1.3.1 (o superiores).
2. **Actualización de libvips:** Garantizar que la biblioteca **libvips** instalada en el servidor esté en la versión **8.13 o superior**, ya que las versiones anteriores no permiten deshabilitar operaciones inseguras y provocan errores de arranque en **Active Storage**.
3. Rotación obligatoria de secretos expuestos: Cambiar e invalidar la secret_key_base**,** la master.key**,** las credenciales de almacenamiento en la nube, las credenciales de bases de datos y todos los tokens de servicios integrados que hayan podido ser exfiltrados.
4. Medidas temporales de contención (Workarounds): En entornos con libvips 8.13 o superior que no puedan actualizar Rails de inmediato, configurar la variable VIPS_BLOCK_UNTRUSTED=true o ejecutar Vips.block_untrusted(true) (requiere ruby-vips 2.2.1 o superior). Si no es posible, eliminar la dependencia de libvips del archivo Gemfile**.**

Prioridad: Crítica.

Ampliar información:

- https://discuss.rubyonrails.org/t/cve-2026-66066-possible-arbitrary-file-read-and-remote-code-execution-in-active-storage-variant-processing/91432
- https://www.herodevs.com/blog-posts/cve-2026-66066-rails-active-storage-arbitrary-file-read-and-rce
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-ruby-on-rails-active-storage-permite-ejecucion-remota-no-autenticada/
- https://thehackernews.com/2026/07/critical-rails-flaw-could-let.html
- https://ethiack.com/info-hub/research/kindarails2shell-rails-rce-cve-2026-66066

MALWARE

NIGHTLEDGER BACKDOOR – NIMBUS MANTICORE (PUERTA TRASERA Y TÚNELES WEBSOCKET PARA CIBERESPIONAJE)

Se identificó una campaña de ciberespionaje atribuida al grupo APT iraní Nimbus Manticore (también conocido como Mirage Kitten, UNC1549, Smoke Sandstorm**,** GalaxyGato y Subtle Snail), dirigida contra los sectores de aviación, telecomunicaciones, gobierno, servicios financieros y Pymes en Medio Oriente, África y Asia del Sur. La operación emplea la puerta trasera NightLedger y las herramientas de tunelización por WebSocket BridgeHead y ArcBridge para convertir los equipos comprometidos en nodos de retransmisión (*covert relays*), permitiendo tunelizar tráfico TCP/SOCKS5 hacia la red interna y evadir los firewalls perimetrales.

Resumen técnico:

- Identificador principal: NightLedger Backdoor / BridgeHead & ArcBridge Tunnelers (Atribuido a Nimbus Manticore / Mirage Kitten).
- Tipo de amenaza: Malware de ciberespionaje, backdoor modular y herramientas de proxying/tunelización SOCKS5 sobre WebSocket.
- Mecanismo de acceso inicial: Spear-phishing altamente personalizado con señuelos de falsas ofertas laborales y portales de videoconferencia suplantados que redirigen a la descarga de archivos maliciosos en servicios de alojamiento de terceros.
- Mecanismo de ejecución y evasión: NightLedger se ejecuta mediante secuestro del orden de búsqueda de DLL (DLL Side-Loading), disfrazándose como SspiCli.dll junto al ejecutable legítimo de Windows AppVShNotify.exe. Crea el mutex A8215357-F99A-44FE-BC65-D8F0434B0C03 para evitar instancias duplicadas.
- Capacidades de NightLedger: Reconocimiento de sistema y usuario, ejecución de procesos, navegación de directorios, captura de pantalla, descarga/carga de archivos vía HTTP POST, finalización de hilos y exfiltración específica del archivo de diagnóstico de dominio C:\Windows\debug\NetSetup.log.
- Capacidades de BridgeHead y ArcBridge (Tunelización): BridgeHead (unbcl.dll) actúa como un proxy SOCKS5 sobre canales HTTPS WebSocket (smartconnect.azurewebsites.net). Cuenta con lógica para evadir proxys empresariales manejando respuestas HTTP 407 mediante la reutilización de credenciales SSO de Windows (Negotiate/NTLM). Además, valida el nombre del usuario de Windows infectado antes de ejecutarse para evitar su análisis en entornos virtuales/sandbox.
- Sistemas y sectores afectados: Entornos Windows en organizaciones de aviación, telecomunicaciones, infraestructura pública y entidades financieras.

Impacto potencial:

- Transformación de estaciones de trabajo en nodos de retransmisión (Relay/Pivoting): Al convertir el equipo infectado en un proxy SOCKS5 encubierto, el atacante tuneliza sus propias herramientas desde el exterior, logrando interactuar con servidores, bases de datos e interfaces internas que no están expuestas a Internet.
- Exfiltración de datos tácticos y logs de infraestructura de dominio: La capacidad de recolectar el archivo NetSetup.log junto con listas de procesos y capturas de pantalla permite al actor malicioso reconstruir la topología de la red Active Directory, identificar nombres de dominio y preparar ataques secundarios de escalada.
- Movimiento lateral encubierto disfrazado de tráfico legítimo: El uso del protocolo WebSocket sobre los puertos estándar HTTPS (443/80) provoca que el tráfico de mando y control (C2) y el tunelización TCP se mezclen con la navegación web convencional de la empresa, complicando su detección en firewalls perimetrales.
- Persistencia evasiva mediante secuestro de binarios del sistema (DLL Side-Loading): Al acoplar la DLL maliciosa a un proceso legítimo del sistema operativo (AppVShNotify.exe), el malware se ejecuta bajo un contexto de proceso confiable, evadiendo la detección de soluciones antivirus tradicionales basadas en firmas.

Recomendaciones de mitigación:

1. Detección y monitoreo de secuestro de carga de DLL (DLL Side-Loading): Configurar reglas de monitoreo en EDR y Sysmon para auditar la ejecución de binarios del sistema como AppVShNotify.exe cuando carguen bibliotecas SspiCli.dll no firmadas o ubicadas en rutas no habituales (%LocalAppData%, carpetas temporales o de aplicaciones de terceros).
2. Inspección profunda de tráfico HTTP/WebSocket y autenticación de proxy: Monitorear peticiones de actualización de protocolo (Upgrade: websocket) iniciadas por procesos que normalmente no requieren comunicación continua, así como detectar reintentos automáticos de autenticación NTLM/Negotiate ante respuestas HTTP 407 dirigidas a dominios externos no categorizados.
3. Micro-segmentación de red y restricción de tráfico interno: Restringir el tráfico de red de las estaciones de trabajo hacia otros segmentos internos o servidores críticos, evitando que un endpoint comprometido pueda ser utilizado como puente para escanear o conectarse a activos internos no autorizados.
4. Fortalecimiento de políticas de concienciación sobre Spear-Phishing: Capacitar a los colaboradores (especialmente en áreas técnicas o corporativas) sobre vectores de ingeniería social basados en ofertas de empleo falsas y enlaces de descarga procedentes de plataformas de videoconferencia no oficiales.

Prioridad: Urgente.

Ampliar información:

- https://vitisecurity.com/stopping-covert-relays-defending-against-sophisticated-apt-backdoors/
- https://underc0de.org/foro/noticias-informaticas-120/nimbus-manticore-despliega-nightledger-y-nuevos-tuneles-websocket/
- https://fixear.net/noticias/nimbus-manticore-convierte-computadoras-comprometidas-en-puentes-secretos-para-espiar-redes-enteras
- https://securelist.com/mirage-kitten-new-tools/120811/
- https://thehackernews.com/2026/07/nimbus-manticore-deploys-nightledger.html

Recomendaciones generales sobre malware:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

PUBLICACIÓN DE PRUEBA DE CONCEPTO (PoC) PARA FALLO CRÍTICO EN CHECK POINT SMARTCONSOLE FACILITA ATAQUES A ESCALA GLOBAL

Investigadores de ciberseguridad han publicado el análisis técnico detallado y un código de Prueba de Concepto (PoC) funcional escrito en Python que demuestra la explotación paso a paso de la vulnerabilidad crítica de omisión de autenticación en Check Point SmartConsole (CVE-2026-16232). La disponibilidad pública de este exploit incrementa drásticamente el nivel de riesgo para las organizaciones que aún no han aplicado las correcciones oficiales emitidas el 22 de julio de 2026, permitiendo que actores de amenazas de menor sofisticación automaticen escaneos y ejecuten compromisos masivos a nivel global.

Resumen técnico:

- Identificador del fallo: CVE-2026-16232 (CVSS v3.1: 9.3 / 9.1).
- Origen de la publicación: Desarrollado y publicado por el equipo de investigación de Rapid7 tras realizar un análisis de causa raíz sobre el flujo de autenticación entre los servicios FWM/CPMI y CPM/DLE de Check Point.
- Mecanismo demostrado en la PoC: El script de prueba valida cómo un atacante remoto no autenticado puede conectarse al servicio FWM/CPMI (puerto TCP 18190), leer el nombre distinguido (DN) SIC del servidor durante el arranque no autenticado, reproducir dicho DN en una solicitud de enlace de aplicación falsificada para obtener un token DLE y, posteriormente, solicitar la generación de un ticket SSO de SmartConsole con privilegios totales de system_admin a través del servicio SOAP de CPM (puerto TCP 19009).
- Evolución del riesgo: Al difundirse el código fuente del exploit en repositorios públicos, el vector de ataque deja de estar limitado a grupos de ciberespionaje avanzados (fase Zero-Day) y pasa a ser incorporado rápidamente en botnets, escáneres automatizados y kits de herramientas de ciberdelincuentes oportunistas.

Impacto potencial:

- Aceleración masiva de ataques automatizados y escaneos de red: La disponibilidad de un script funcional reduce a cero la barrera técnica para explotar la vulnerabilidad, aumentando drásticamente los intentos de intrusión contra cualquier servidor de gestión expuesto.
- Compromiso no autenticado del servidor de gestión central: La ejecución exitosa de la PoC otorga una sesión activa con derechos de administrador del sistema (system_admin), permitiendo la modificación remota de objetos, reglas de firewall y políticas de seguridad corporativas.
- Inactivación de defensas perimetrales y facilitación de ransomware: El control administrativo del servidor de gestión faculta a los atacantes a desplegar configuraciones permisivas en los Security Gateways administrados, facilitando el movimiento lateral y la propagación de ransomware en la red interna.
- Evasión de mecanismos de autenticación tradicionales: Al generar un ticket SSO internamente válido mediante la falsificación de la sesión de aplicación, el ataque no activa alertas de fuerza bruta ni requiere la interceptación de credenciales de usuario o tokens MFA.

Recomendaciones para mitigar el riesgo:

1. Aplicación inmediata de los Jumbo Hotfixes oficiales: Actualizar sin demora los servidores de gestión a las versiones corregidas por el fabricante (R81.20 Jumbo Hotfix Take 158, R82 Take 118, R82.10 Take 36 o superiores) para implementar las validaciones estrictas del DN en los certificados de cliente.
2. Restricción estricta de Clientes de Confianza (Trusted Clients): Configurar el parámetro de clientes GUI en SmartConsole para permitir el acceso únicamente desde direcciones IP o subredes explícitamente autorizadas, eliminando cualquier regla genérica basada en Any.
3. Bloqueo perimetral de interfaces y puertos de gestión: Asegurar que los puertos TCP 18190 y TCP 19009 no estén expuestos directamente a la Internet pública, canalizando el acceso administrativo exclusivamente a través de redes de gestión aisladas, VPNs corporativas o plataformas ZTNA.
4. Ejecución de validaciones defensivas en entornos de pruebas: Utilizar la PoC publicada únicamente en entornos de laboratorio autorizados para verificar que los parches hayan sido aplicados correctamente y ajustar las reglas de correlación en herramientas SIEM/EDR ante posibles firmas de explotación.

Prioridad: Urgente.

Ampliar Información:

- https://owltech.com.ar/alerta-critica-descubren-fallo-de-seguridad-en-check-point-smartconsole/
- https://www.cert.gov.py/vulnerabilidades-en-productos-check-point-2/
- https://blog.elhacker.net/2026/07/publican-poc-para-el-bypass-de.html
- https://thehackernews.com/2026/07/rapid7-releases-poc-for-exploited-check.html
- https://csirt.telconet.net/comunicacion/boletines-servicios/bypass-de-autenticacion-en-check-point-smartconsole-explotado-activamente/