GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2326

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-2026-25089 – FORTINET FORTISANDBOX (INYECCIÓN DE COMANDOS DEL SISTEMA OPERATIVO DE SEGUNDO ORDEN EN INTERFAZ WEB)

Se ha divulgado una vulnerabilidad crítica de inyección de comandos en el sistema operativo que afecta a la interfaz de administración web de las soluciones de sandboxing de Fortinet. El fallo permite a atacantes remotos no autenticados ejecutar comandos arbitrarios en la infraestructura subyacente, lo cual representa un riesgo severo para los entornos empresariales que confían en estos appliances para el análisis dinámico y la contención de amenazas complejas.

Resumen técnico:

- Identificador principal: CVE-2026-25089 (Advisory ID: FG-IR-26-141).
- Severidad: Crítica (Puntaje base de 9.1 en CVSS v3.1 / Hasta 9.8 en evaluaciones de impacto según métricas de infraestructura expuesta).
- Causa raíz: Una neutralización inadecuada de elementos especiales dentro de los comandos del sistema operativo (CWE-78) en el componente de la interfaz gráfica de usuario (GUI). El fallo se localiza específicamente en la validación de datos de la característica "start VNC".
- Mecanismo de falla: Un atacante remoto sin credenciales válidas envía una solicitud HTTP maliciosa especialmente diseñada que inyecta datos JSON manipulados hacia el endpoint de la función "start VNC". Al procesarse, el sistema incurre en una inyección de segundo orden: la carga útil se almacena o procesa inicialmente en un contexto de la aplicación y posteriormente se ejecuta dentro del contexto del sistema operativo subyacente de la interfaz web, evadiendo los filtros de sanitización tradicionales.
- Estado de explotación: Divulgación pública coordinada el 9 de junio de 2026 tras un reporte interno del equipo de PSIRT de Fortinet. Al momento de la emisión de las alertas no se registran reportes de explotación activa en el entorno real (in the wild), pero la disponibilidad de detalles de la arquitectura técnica eleva el riesgo de ingeniería inversa a corto plazo.
- Versiones afectadas: * FortiSandbox en versiones 5.0.0 hasta 5.0.5, y versiones 4.4.0 hasta 4.4.8.
  - FortiSandbox Cloud en versiones 5.0.4 hasta 5.0.5.
  - FortiSandbox PaaS en versiones 5.0.4 hasta 5.0.5.
  - Las ramas FortiSandbox 5.2, FortiSandbox Cloud 5.2 y FortiSandbox PaaS 23.4 se encuentran nativamente protegidas y no son afectadas).

Impacto potencial:

- Ejecución remota de comandos arbitrarios sin autenticación: Al no requerir credenciales de acceso a la GUI, cualquier atacante con visibilidad de red sobre el endpoint puede tomar control operativo del software base e inyectar instrucciones dañinas de forma directa.
- Compromiso de información táctica y muestras de malware: Debido a que estos sistemas custodian archivos bajo sospecha, reportes de comportamiento de amenazas e integraciones clave de seguridad, un acceso no autorizado expone datos analizados altamente confidenciales de la organización.
- Pivoteo y movimiento lateral hacia la red interna: Al encontrarse profundamente acoplados en la topología de la infraestructura para recibir muestras automatizadas desde firewalls, EDRs y servidores de correo, un compromiso exitoso en el sandbox provee un puente ideal para saltar a otros segmentos críticos de la red corporativa.
- Evasión de firmas estáticas y auditorías inmediatas: Al tratarse de un ataque de "segundo orden", la petición HTTP inicial con la carga JSON puede ser almacenada de forma aparentemente benigna antes de gatillar la ejecución en memoria, dificultando su detección en tiempo real mediante reglas tradicionales de WAF perimetrales.

Recomendaciones de mitigación:

1. Actualización inmediata a compilaciones de seguridad oficiales: Se urge a los equipos de administración a aplicar los parches del fabricante migrando de manera prioritaria a las versiones FortiSandbox 5.0.6 o superior, FortiSandbox 4.4.9 o superior, FortiSandbox Cloud 5.0.6 o superior y FortiSandbox PaaS 5.0.6 o superior.
2. Restricción estricta de la exposición en el perímetro: Configurar políticas de firewall perimetral para asegurar que la interfaz gráfica de usuario (Web UI) de administración de los appliances de diagnóstico no esté expuesta directamente a la red pública de Internet.
3. Aislamiento en zonas de red de gestión dedicadas (VLANs de O&M): Confinar el tráfico administrativo del FortiSandbox empleando listas de control de acceso (ACLs) estrictas o pasarelas de acceso de confianza cero (ZTNA), requiriendo el uso obligatorio de canales VPN y autenticación multifactor (MFA) para alcanzar la interfaz.
4. Auditoría y correlación de telemetría HTTP en la GUI: Implementar reglas de monitorización activa en las soluciones SIEM para identificar solicitudes HTTP malformadas, comportamientos anómalos o ráfagas de payloads JSON sospechosos orientados específicamente hacia las funcionalidades Web de VNC afectadas.

Prioridad: Crítica.

Ampliar información:

- https://gbhackers.com/fortinet-fortisandbox-vulnerability-2/#google_vignette
- https://www.fortiguard.com/psirt/FG-IR-26-141
- https://thehackernews.com/2026/06/ivanti-fortinet-and-sap-release-patches.html
- https://www.heise.de/en/news/Fortinet-closes-command-injection-vulnerability-in-FortiSandbox-and-more-11327025.html
- https://www.securityweek.com/critical-vulnerabilities-patched-in-fortinet-ivanti-products/

CVE-2026-5027 – LANGFLOW (SALTO DE DIRECTORIO Y EJECUCIÓN REMOTA DE CÓDIGO NO AUTENTICADA - RCE)

Se ha detectado la explotación activa en el entorno real de una vulnerabilidad de alta severidad en Langflow, la plataforma de código abierto de bajo código utilizada para la construcción de aplicaciones y agentes de Inteligencia Artificial. El fallo de salto de directorio (Path Traversal) puede ser encadenado con las configuraciones por defecto del sistema para permitir a atacantes remotos no autenticados escribir archivos arbitrarios en el servidor de destino, logrando la ejecución remota de código (RCE) y el compromiso total de las herramientas de desarrollo de IA.

Resumen técnico:

- Identificador principal: CVE-2026-5027.
- Severidad: Alta / Crítica (Puntaje base de 8.8 en CVSS v3.1; clasificado bajo la métrica de limitación inadecuada de rutas de acceso CWE-22).
- Causa raíz: Una falta de sanitización y validación estricta sobre el parámetro filename dentro de los datos de formularios multipart recibidos en el endpoint POST /api/v2/files.
- Mecanismo de falla: Debido a que Langflow viene configurado de fábrica con la función de inicio de sesión automático sin credenciales (unauthenticated auto-login), un atacante remoto solo requiere emitir una única petición inicial para adquirir un token de sesión legítimo. Posteriormente, abusa de dicho token enviando una solicitud HTTP estructurada hacia el endpoint de carga de archivos, inyectando secuencias de escape de directorio tradicionales (../) en el nombre del archivo. Esto le otorga la capacidad de evadir la carpeta temporal restringida y escribir componentes maliciosos en cualquier ubicación del sistema de archivos, derivando en la ejecución remota de comandos.
- Estado de explotación: En explotación activa detectada por honeypots globales a inicios de junio de 2026. Los análisis de telemetría confirman que los atacantes están automatizando el escaneo sobre las aproximadamente 7,000 instancias de Langflow expuestas públicamente en Internet (principalmente en Norteamérica) para depositar archivos de prueba y cargas útiles.
- Versiones afectadas: Todas las implementaciones de Langflow anteriores a la versión 1.9.0, así como las instalaciones que dependan del paquete subyacente langflow-base en versiones previas a la 0.8.3.

Impacto potencial:

- Ejecución remota de código sin interacción del usuario: Al no demandar credenciales de acceso ni pasos de validación por parte de un operador, el ataque permite a actores maliciosos tomar control directo del proceso del sistema operativo que aloja la suite de IA de forma completamente remota.
- Exfiltración de secretos, variables de entorno y API Keys: Al comprometer la instancia de desarrollo, los atacantes adquieren acceso directo a los archivos de configuración locales (como .env o bases de datos .db), lo que expone tokens de acceso de producción de proveedores de LLMs, credenciales de nubes y claves criptográficas de la organización.
- Manipulación y envenenamiento de canalizaciones de IA (RAG): Un atacante con privilegios de escritura de archivos puede adulterar de manera silenciosa la lógica de los flujos de trabajo, los prompts del sistema o los conectores de bases de conocimiento (Retrieval-Augmented Generation), forzando a los agentes de IA corporativos a entregar respuestas maliciosas o a filtrar información sensible.
- Persistencia avanzada dentro del entorno de desarrollo: La capacidad de escribir en rutas arbitrarias del disco permite a los atacantes plantar scripts de persistencia en carpetas de inicio automático o modificar librerías legítimas de Python, garantizando el acceso a largo plazo incluso si el servicio de la aplicación es reiniciado.

Recomendaciones de mitigación:

1. Actualización forzada a la versión de producción más reciente: Se urge a los equipos de ingeniería y seguridad a migrar de manera inmediata a la versión Langflow 1.10.0 (o superior), o en su defecto asegurar la aplicación de los parches correspondientes mediante la actualización de langflow-base a la versión 0.8.3 y la aplicación principal a la versión 1.9.0.
2. Desactivación obligatoria del inicio de sesión automático: Modificar las variables de entorno de ejecución de la plataforma para deshabilitar la directiva de auto-login sin credenciales por defecto, forzando de forma estricta el paso por un portal de autenticación robusto antes de exponer cualquier endpoint de la API.
3. Aislamiento perimetral y mitigación de la exposición pública: Restringir de manera contundente el acceso a las interfaces gráficas y APIs de Langflow desde redes públicas. Se recomienda confinar estas herramientas exclusivamente dentro de la red local corporativa o exigir su consumo a través de pasarelas de red privadas virtuales (VPN) o políticas Zero Trust (ZTNA).
4. Implementación de firmas y monitoreo de secuencias de escape: Configurar reglas de inspección a nivel de Web Application Firewall (WAF) o sistemas de detección de intrusiones (IDS) orientadas a bloquear peticiones HTTP hacia el endpoint /api/v2/files que contengan caracteres codificados o en texto plano de salto de directorio (../ o %2e%2e%2f).

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/06/unpatched-langflow-flaw-cve-2026-5027.html
- https://www.mallory.ai/stories/019eb249-8374-767e-b12b-c7be9be0c2d7
- https://www.bleepingcomputer.com/news/security/path-traversal-flaw-in-ai-dev-platform-langflow-exploited-in-attacks/
- https://db.gcve.eu/vuln/CVE-2026-5027

CVE-2026-11645 – CHROME V8 ENGINE (LECTURA Y ESCRITURA FUERA DE LÍMITES Y EJECUCIÓN REMOTA DE CÓDIGO - ZERO-DAY)

Google ha emitido una actualización de seguridad de emergencia para corregir una vulnerabilidad de alta gravedad en su motor JavaScript y WebAssembly V8, el cual es utilizado por Google Chrome y todo el ecosistema de navegadores basados en Chromium. La falla está siendo explotada activamente en el entorno real (in the wild) como un ataque Zero-Day, lo que permite a atacantes remotos comprometer las sesiones de navegación de los usuarios con solo forzar el procesamiento de una página web maliciosa.

Resumen técnico:

- Identificador principal: CVE-2026-11645.
- Severidad: Alta / Crítica (Puntaje base de 8.8 en CVSS v3.1; clasificado bajo las categorías de lectura y escritura fuera de límites de memoria CWE-125 y CWE-787).
- Causa raíz: Un defecto de lógica en el compilador Just-In-Time (JIT) de V8, conocido como TurboFan. Al realizar optimizaciones especulativas de rendimiento, el compilador elimina de forma errónea las comprobaciones de límites (boundary checks) en operaciones críticas sobre arrays de JavaScript.
- Mecanismo de falla: Un atacante diseña un script de JavaScript ofuscado dentro de una página HTML manipulada. Al ser renderizada por el navegador, el código engaña a TurboFan para operar fuera de los límites de memoria asignados al array. Esto genera dos primitivas de ataque consecutivas: primero, una lectura fuera de límites que filtra punteros internos del motor y direcciones físicas reales, logrando neutralizar por completo la protección ASLR (aleatorización del espacio de direcciones); segundo, una escritura fuera de límites que corrompe los punteros de funciones en memoria, desviando el flujo de ejecución del proceso hacia una carga útil (payload) arbitraria bajo control del atacante.
- Estado de explotación: Explotación activa global confirmada. Se trata del quinto Zero-Day detectado y parchado en Google Chrome en lo que va del año 2026. Los vectores principales identificados involucran campañas de spear-phishing dirigido y ataques de tipo watering hole (sitios web legítimos de uso corporativo que han sido previamente inyectados con el script malicioso).
- Versiones afectadas: Google Chrome en versiones anteriores a la 149.0.7827.103 en sistemas operativos Windows y macOS, y anteriores a la versión 149.0.7827.102 en plataformas Linux. El fallo afecta de forma heredada a cualquier navegador basado en el núcleo Chromium (Microsoft Edge, Brave, Opera, Vivaldi) y a marcos de desarrollo como Electron que empaquetan instancias vulnerables de V8.

Impacto potencial:

- Ejecución remota de código (RCE) en el proceso de renderizado: Permite a un atacante tomar control operativo inmediato sobre la pestaña o proceso del navegador que procesa la web maliciosa, ejecutando comandos nativos de forma invisible en milisegundos y sin necesidad de que el usuario descargue o instale archivos.
- Robo masivo de cookies de sesión, credenciales y tokens corporativos: Al comprometer la memoria activa del navegador, el atacante puede extraer bases de datos de contraseñas guardadas, tokens JWT de autenticación activa y cookies de sesión de plataformas críticas de la empresa (CRMs, ERPs, repositorios de código y consolas de administración en la nube), permitiendo un secuestro posterior de cuentas (Account Takeover).
- Evasión de mecanismos de protección de memoria de nivel de sistema: La capacidad de lectura en memoria anula de manera efectiva la protección ASLR de las estaciones de trabajo, debilitando la postura general del endpoint y facilitando ataques complementarios dirigidos a la infraestructura de software.
- Puente para el escape completo de sandbox del sistema operativo: Aunque la ejecución inicial de código ocurre dentro del entorno de aislamiento (sandbox) del navegador, un actor de amenazas sofisticado puede encadenar este exploit con vulnerabilidades del kernel del sistema operativo o del proceso broker de Chrome para obtener privilegios de administrador (root / SYSTEM) en el equipo afectado.

Recomendaciones de mitigación:

1. Actualización inmediata y reinicio mandatorio del navegador: Se urge a implementar de forma inmediata el parche de seguridad en los endpoints mediante la descarga de Chrome versión 149.0.7827.103 o posterior (o la versión correspondiente .102 en Linux). Es imperativo que los usuarios utilicen la opción "Reiniciar / Relaunch" del navegador, ya que el parche no se cargará en la memoria activa hasta que el proceso de la aplicación se inicialice por completo.
2. Auditoría de políticas de grupo (GPO) para actualizaciones automatizadas: Validar mediante directivas de Active Directory que el servicio corporativo de actualizaciones de Google (Google Update) no esté deshabilitado ni bloqueado por reglas de firewall perimetral o proxies internos, garantizando el despliegue automático del parche en la totalidad del parque informático.
3. Actualización del ecosistema Chromium y dependencias Electron: Monitorear y exigir la actualización oportuna de navegadores secundarios aprobados en la organización (como Microsoft Edge o Brave), así como de aplicaciones de escritorio basadas en Electron (Slack, Microsoft Teams, VS Code), que consuman componentes JIT del motor V8 afectado.
4. Monitoreo conductual mediante soluciones EDR / XDR: Configurar y ajustar las herramientas de detección en el endpoint para identificar comportamientos anómalos originados por los procesos de renderizado del navegador (chrome.exe, msedge.exe), tales como la instanciación de shells de comandos (cmd.exe, powershell.exe), inyecciones de memoria sospechosas o intentos inusuales de lectura sobre archivos de configuración locales.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/06/chrome-v8-zero-day-cve-2026-11645.html
- https://csirt.telconet.net/comunicacion/boletines-servicios/actualizacion-de-seguridad-en-google-chrome-corrige-vulnerabilidad-zero-day-en-motor-v8/
- https://hdti.cl/blog/chrome-zero-day-cve-2026-11645-v8-exploit-activo-que-hacer/
- https://www.helpnetsecurity.com/2026/06/09/google-chrome-zero-day-cve-2026-11645/
- https://blog.enhacke.com/zero-day-en-chrome-vulnerabilidad-critica-cve-2026-11645-descubierta/

MALWARE

CAMPAÑA HADES – INFECTOR AUTOMÁTICO Y ROBO MASIVO DE CREDENCIALES EN LA CADENA DE SUMINISTRO DE PYPI

Se ha detectado una campaña coordinada y de alta sofisticación de ataque a la cadena de suministro dentro del índice de paquetes de Python (PyPI), denominada "Hades Campaign". Esta amenaza, vinculada directamente a la evolución del linaje de malware Shai-Hulud / Miasma, ha comprometido al menos 19 paquetes legítimos (distribuidos en 37 archivos wheel maliciosos) enfocados principalmente en herramientas de desarrollo, Inteligencia Artificial, Aprendizaje Automático (ML) y bioinformática. El peligro crítico de este malware radica en su capacidad para autoejecutarse de forma silenciosa inmediatamente tras la instalación, procediendo a un raspado agresivo de credenciales en la nube y secretos empresariales.

Resumen técnico:

- Tipo de amenaza: Código malicioso de robo de información (Infostealer) con capacidades de extorsión (Wiper) y autopropagación de tipo gusano (Worm).
- Mecanismo de entrada silencioso: El vector aprovecha archivos con la extensión *-setup.pth incrustados maliciosamente dentro de los paquetes comprimidos corporativos (wheels). El módulo nativo site de Python procesa de forma automática estos archivos de ruta en el arranque del intérprete. Si el archivo contiene líneas con la instrucción import, las ejecuta de inmediato. En otros clústeres de la campaña, la carga se inyecta como un import hook ofuscado de una sola línea dentro del archivo __init__.py. Esto provoca que el malware se active con solo invocar el entorno de Python, sin necesidad de que el usuario haga un import explícito de la librería comprometida.
- Cadena de ejecución híbrida (Python → Bun → JS): Tras activarse, el script de Python descarga de forma transparente el entorno de ejecución de JavaScript independiente Bun (versiones v1.3.13/v1.3.14) en formato ZIP directamente desde los repositorios de GitHub. Al desempaquetarlo, utiliza este motor para ejecutar un payload denominado _index.js que contiene 16 componentes funcionales cifrados. Este enfoque multi-entorno permite al atacante ejecutar lógicas complejas de evasión y robo de datos sin depender de que el sistema cuente con Node.js preinstalado, evadiendo la telemetría de monitoreo tradicional.
- Raspado avanzado de memoria de procesos: Introduce componentes avanzados a nivel de sistema operativo diseñados para leer de forma directa la memoria activa de las máquinas y recolectar credenciales volátiles (apuntando con especial énfasis al proceso de ejecución del agente Runner.Worker de GitHub Actions). El malware implementa técnicas personalizadas según la plataforma: en Linux accede a través de /proc/{pid}/mem, en macOS abusa de las APIs del kernel de Mach y en Windows emplea la llamada nativa de la API ReadProcessMemory.

- Evasión de defensas y técnicas de camuflaje anti-IA: Para eludir los escáneres automáticos de código basados en Inteligencia Artificial (LLMs), el payload inyecta fragmentos de prompt injection en texto plano estructurados para engañar al analizador y forzarlo a clasificar el paquete como "seguro". Adicionalmente, el malware simula tráfico de red benigno enviando peticiones señuelo hacia los endpoints de Anthropic AI para confundir las defensas perimetrales, y suspende toda actividad destructiva o de robo si detecta una configuración regional de idioma ruso (Russian locale).
- Ecosistemas y paquetes afectados: Afecta a librerías populares en bioinformática y flujos de IA/ML, tales como: ensmallen, embiggen, mflux-streamlit, nhmpy, gpsea, pyphetools, dynamo-release, spateo-release, coolbox, ufish, pantheon-agents, executor-engine, magique-ai, entre otras.

Impacto potencial:

- Exfiltración masiva de secretos corporativos y de desarrollo: El malware extrae de manera automatizada claves de acceso y tokens de nubes públicas (AWS, Azure, GCP), tokens de Kubernetes, credenciales de publicación en registros globales (PyPI, npm, RubyGems, JFrog), tokens de acceso personal (PAT) de GitHub, tokens de CircleCI, credenciales de Vault, llaves de infraestructura SSH, configuraciones de Docker e historiales de consola, lo cual desestabiliza por completo el control de acceso institucional.
- Mecanismo de extorsión destructivo mediante borrado de datos (Wiper): Como una inédita medida de contención contra el equipo de seguridad, el malware instala un servicio persistente en segundo plano llamado gh-token-monitor. Este componente supervisa el estado de validez de los tokens robados de GitHub; si detecta que el desarrollador o el administrador revoca la clave expuesta, el daemon activa un comando de destrucción total (rm -rf ~/; rm -rf ~/Documents), eliminando de forma irrecuperable los archivos y el directorio home de la víctima.
- Autopropagación colateral en la cadena de suministro: Si los tokens de GitHub o las identidades de publicación exfiltradas poseen permisos de escritura, el malware automatiza la inyección de sus propios componentes dañinos en los repositorios de la empresa o empuja actualizaciones corruptas hacia PyPI abusando de las relaciones de confianza OIDC (OpenID Connect), convirtiendo el sistema en un vector que infecta de forma exponencial a los clientes de la organización.
- Backdoors en asistentes de IA locales y persistencia avanzada: El malware inyecta de forma silenciosa ganchos de código malicioso en los directorios de espacios de trabajo locales. Estas puertas traseras están diseñadas para activarse cuando los proyectos de desarrollo son abiertos en IDEs o procesados por asistentes de codificación de Inteligencia Artificial (tales como Anthropic Claude, OpenAI Codex, Google Gemini, Microsoft Copilot, Cline, Aider o Tabby), garantizando el acceso continuo de los atacantes a largo plazo.

Recomendaciones de mitigación:

1. Identificación, auditoría y remoción inmediata de paquetes comprometidos: Es prioritario realizar un inventario urgente de los entornos de desarrollo de software, estaciones locales de ingenieros y agentes de construcción de código de la compañía para detectar las versiones afectadas de los 19 paquetes comprometidos. Se debe realizar la eliminación forzada de los paquetes y buscar manualmente archivos anómalos *-setup.pth o modificaciones de una sola línea en módulos __init__.py dentro de las carpetas de site-packages.
2. Aislamiento de red mandatorio antes de la rotación de credenciales: Debido al comportamiento agresivo del componente de extorsión wiper (gh-token-monitor), NO se deben revocar ni rotar los tokens de GitHub o llaves de nube mientras la estación de trabajo afectada esté conectada a la red. Primero se debe desconectar y aislar por completo el host comprometido del entorno para cortar la comunicación del malware con las APIs de control, y solo entonces proceder con la revocación masiva y regeneración de secretos desde un equipo limpio.
3. Caza activa de artefactos de persistencia locales (Threat Hunting): Configurar búsquedas proactivas de indicadores de compromiso (IoCs) para localizar los daemons instalados en segundo plano y los archivos de bloqueo creados por la campaña, rastreando las siguientes rutas clave: En sistemas Linux: ~/.config/systemd/user/update-monitor.service y ~/.config/systemd/user/gh-token-monitor.service, en sistemas macOS: ~/Library/LaunchAgents/com.user.gh-token-monitor.plist y Archivos de bloqueo temporales: /tmp/.bun_ran y /tmp/tmp.0144018410.lock.

4 Reconstrucción y endurecimiento de entornos: Ante las técnicas de raspado de memoria y persistencia empleadas por Hades, se recomienda realizar un reimage completo de las máquinas de desarrollo y servidores CI/CD comprometidos. Adicionalmente, implementar soluciones de endurecimiento de pipelines, como StepSecurity Harden-Runner, con filtrado de salida de red (Egress Filtering)

Prioridad: Urgente.

Ampliar información:

- https://www.securityweek.com/over-100-npm-pypi-packages-hit-in-new-shai-hulud-supply-chain-attacks/
- https://socradar.io/blog/shai-hulud-hades-pypi-campaign/
- https://www.rescana.com/post/active-exploitation-alert-hades-pypi-supply-chain-attack-poisons-19-python-packages-with-bun-based-credential-stealer
- https://thehackernews.com/2026/06/hades-pypi-attack-19-packages-poisoned.html
- https://orca.security/resources/blog/hades-pypi-supply-chain-attack/

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

EXPLOTACIÓN ACTIVA DE VULNERABILIDAD CRÍTICA DE OMISIÓN DE AUTENTICACIÓN EN CHECK POINT VPN (CVE-2026-50751)

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha incorporado de emergencia la vulnerabilidad CVE-2026-50751 a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), tras confirmarse incidentes globales en el entorno real donde actores de amenazas abusan de este fallo perimetral para infiltrarse en redes corporativas. El fallo afecta a las soluciones de acceso remoto de Check Point, y su explotación exitosa en al menos un caso confirmado ha permitido el despliegue posterior de ataques operados por afiliados del grupo de ransomware Qilin, lo que eleva la alerta al máximo nivel operativo.

Resumen técnico:

- Identificador principal: CVE-2026-50751 (Flallos complementarios identificados en la misma revisión de código bajo el registro CVE-2026-50752).
- Severidad: Crítica (Puntaje base de 9.3 en CVSS v3.1 / Clasificado bajo la categoría de autenticación incorrecta CWE-287).
- Causa raíz: Una falla latente en el flujo lógico de validación de certificados digitales durante el intercambio de claves en el protocolo IKEv1, un estándar de cifrado antiguo y obsoleto que muchas organizaciones mantienen activo por motivos de compatibilidad hacia atrás.
- Mecanismo de falla: Un atacante remoto no autenticado envía paquetes de negociación IKEv1 específicamente manipulados hacia el Security Gateway expuesto. Al procesarse, la lógica defectuosa del firewall valida de forma errónea la identidad de la sesión, permitiendo al atacante saltarse por completo las solicitudes de credenciales y establecer un túnel VPN de acceso remoto totalmente operativo sin poseer contraseñas de usuario legítimas.
- Condiciones para la explotación: El entorno es vulnerable únicamente si se cumplen simultáneamente cuatro factores: 1) Las funciones de Remote Access VPN o Mobile Access están activas. 2) IKEv1 está habilitado para estos accesos. 3) El gateway está configurado para aceptar conexiones de clientes de acceso remoto heredados (Legacy). 4) La puerta de enlace no tiene configurada la exigencia de un certificado de máquina obligatorio para validar el endpoint.
- Estado de explotación: En explotación activa desde junio de 2026, con indicios de ataques dirigidos desde mayo de 2026. Los atacantes emplean VPS ubicados en el mismo país de las víctimas para evadir alertas geográficas, utilizando Rclone para el robo de datos y el protocolo Tox para coordinar extorsiones.Versiones afectadas: * Security Gateways: Versiones R82.10 (Jumbo Hotfix Take 19 o inferior), R82 (Jumbo Hotfix Take 103 o inferior) y R81.20 (Jumbo Hotfix Take 141 o inferior), sistemas en Fin de Soporte (EOS): Ramas de software sin mantenimiento oficial que permanecen altamente vulnerables, incluyendo R81.10, R81 y R80.40 y Firewalls integrados Spark (Pymes/MSPs): Versiones R80.20.X, R81.10.X y R82.00.X.

Impacto potencial:

- Acceso perimetral no autorizado y bypass total de contraseñas: Permite a actores de amenazas externos derribar la primera línea de defensa de la organización, estableciendo una sesión de red confiable dentro de la infraestructura perimetral sin levantar sospechas iniciales de inicios de sesión anómalos o ataques de fuerza bruta.
- Despliegue masivo de Ransomware e interrupción del negocio: La asociación directa de esta campaña con el ecosistema de ransomware Qilin implica que, una vez dentro de la red, los intrusos buscarán comprometer los controladores de dominio y deshabilitar copias de seguridad para ejecutar un cifrado destructivo a gran escala sobre servidores críticos.
- Exfiltración de información confidencial mediante herramientas legítimas: Al establecer la sesión de VPN, los atacantes abusan de binarios de transferencia como Rclone para sustraer bases de datos, documentación interna y propiedad intelectual hacia repositorios externos controlados por el operador (como Kaupo Cloud, Shock Hosting o Vultr), materializando incidentes graves de brechas de datos antes de que se perciba el ataque.
- Movimiento lateral acelerado e instalación de implantes ELF: Al consolidar el acceso a nivel de túnel de red, los vectores observados ejecutan de inmediato solicitudes HTTP internas para descargar y sembrar binarios de Linux maliciosos (archivos ELF) en appliances adyacentes, construyendo canales secundarios de comando y control (C2) que dificultan la contención perimetral estándar.

Recomendaciones para mitigar el riesgo:

1. Instalación inmediata de parches oficiales y Hotfixes del fabricante: Se insta a los administradores de redes a aplicar los hotfixes de seguridad de Check Point sin dilación, asegurando elevar los Security Gateways por encima de Jumbo Hotfix Take 19 (en R82.10), Take 103 (en R82) y Take 141 (en R81.20). Aquellas infraestructuras operando en ramas obsoletas (R80.40/R81/R81.10) deben ser migradas de urgencia a versiones con soporte vigente.
2. Desactivación estricta del protocolo obsoleto IKEv1: Modificar la configuración global de las propiedades de autenticación de Remote Access VPN y Mobile Access en el SmartConsole para deshabilitar por completo el uso de IKEv1, forzando de manera mandatoria y exclusiva la utilización del protocolo moderno y seguro IKEv2 para todas las conexiones entrantes.
3. Remoción de clientes heredados y obligatoriedad de certificados de máquina: Revocar los permisos que aceptan conexiones desde clientes de acceso remoto antiguos (Legacy Remote Access Clients). Paralelamente, se debe robustecer la directiva de acceso exigiendo de forma obligatoria la validación de un Certificado de Máquina válido emitido por la CA corporativa para autorizar cualquier intento de conexión perimetral.
4. Auditoría forense retroactiva de registros y activación de firmas IPS: Programar un análisis forense exhaustivo de los logs de auditoría y registros de conexión de los Gateways con una ventana retrospectiva que inicie desde el 7 de mayo de 2026 para identificar accesos VPN anómalos, túneles levantados sin contraseñas asociadas o transferencias salientes atípicas. Asimismo, se debe asegurar la actualización inmediata de las firmas del módulo IPS de Check Point asociadas al advisory del fabricante.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews.com/2026/06/critical-check-point-vpn-flaw-exploited.html
- https://socprime.com/es/blog/cve-2026-50751-explotacion-en-ataques-dirigidos-de-omision-de-autenticacion-en-check-point-vpn/
- https://csirt.telconet.net/comunicacion/boletines-servicios/omision-de-autenticacion-en-check-point-remote-access-vpn-y-mobile-access-mediante-ikev1/
- https://www.sseguras.com/noticias/noticias-y-eventos/2026-06-08-actualizacion-de-seguridad-requerida-para-check-point-vpn
- https://unaaldia.hispasec.com/cisa-impone-un-parche-expres-para-un-fallo-critico-en-la-vpn-de-check-point-explotado-por-qilin/
- https://www.helpnetsecurity.com/2026/06/08/check-point-cve-2026-50751-qilin-ransomware/