

GammaCS-CERT
By Gamma Ingenieros



Boletín de Ciberseguridad Semanal

Edición °3926



BOLETÍN DE CIBERSEGURIDAD SEMANTAL

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 para nuestros 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

MODEL CONTEXT PROTOCOL (MCP) PYTHON SDK – VULNERABILIDAD ALTA DE OMISIÓN DE VALIDACIÓN DE EMISOR PERMITE EL ROBO DE CREDENCIALES OAUTH Y SECUESTRO DE SESIÓN (GHSA-qx49-fqc8-xw99)

Los mantenedores de Model Context Protocol (MCP) han publicado actualizaciones de seguridad para corregir una vulnerabilidad de severidad alta en el SDK oficial de Python para MCP. El fallo se debe a la falta de validación del emisor (issuer) en las rutas de respaldo (fallback) del proceso de descubrimiento OAuth. Un servidor MCP malicioso o comprometido puede forzar al cliente a enviar el secreto de cliente (client_secret), el código de autorización y la clave de prueba PKCE hacia un endpoint de tokens controlado por el atacante, permitiendo obtener acceso no autorizado a servicios de identidad integrados.

Resumen técnico:

- Identificador principal: GHSA-qx49-fqc8-xw99 (Sin CVE asignado).
- Severidad: Alta (CVSS v3.1: 7.5).
- Causa raíz: Validación insuficiente de la autenticidad de los datos / Omisión de verificación de emisor en el descubrimiento de metadatos del servidor de autorización (CWE-345 / RFC 8414).
- Mecanismo de falla:
- Al requerir autenticación OAuth, el cliente SDK solicita al servidor MCP la ubicación del servidor de autorización. Si un servidor MCP malicioso responde con un error HTTP 404 o 403 (insufficient_scope) en el endpoint /.well-known/oauth-authorization-server, el SDK utiliza una ruta de respaldo que consulta la configuración directamente al propio servidor MCP.
- En esta ruta de respaldo, el SDK omite la validación del emisor (issuer) al no estar configurada la URL del servidor de autorización, permitiendo que el servidor atacante declare falsamente a un proveedor de identidad legítimo (como Google, Okta, Azure AD o Keycloak) pero especifique un endpoint de tokens bajo su control.
- El usuario o proceso se autentica legítimamente en la página del proveedor real, pero tras la aprobación, el SDK envía el client_secret, el código de autorización y el code_verifier de PKCE al endpoint de tokens controlado por el atacante.
- El atacante canjea estas credenciales ante el proveedor de identidad legítimo y obtiene un token de acceso válido con todos los permisos otorgados a la aplicación cliente.
- Estado de explotación: Divulgada oficialmente el 28 de septiembre de 2026 (corregida en las versiones 1.30.0 y 2.2.0). Se cuenta con prueba de concepto (PoC) técnica documentada; no se registra evidencia de explotación activa en el entorno real previa a la divulgación.
- Versiones afectadas: MCP Python SDK (paquete mcp) en versiones 1.9.1 a 1.29.1 y 2.0.0 a 2.1.1.

Impacto potencial:

- Robo y exfiltración de credenciales OAuth sensibles: Permite a un atacante interceptar el secreto de cliente (client_secret), códigos de autorización, claves de prueba PKCE y aserciones JWT firmadas.
- Persistencia prolongada mediante credenciales de larga duración: Debido a que el client_secret es una credencial estática y duradera, el compromiso persiste de forma indefinida hasta que se realice una rotación explícita en el proveedor de identidad.
- Afectación silenciosa e indetectable en flujos máquina a máquina (M2M): Impacta de forma crítica a componentes desatendidos (ClientCredentialsOAuthProvider y PrivateKeyJWTAuthProvider), cosechando credenciales en agentes de IA y flujos de trabajo sin generar alertas o solicitudes de inicio de sesión visibles.
- Apropiación de cuentas y acceso no autorizado a servicios corporativos: Otorga al atacante la capacidad de generar tokens válidos ante el proveedor de identidad real (Okta, Azure AD, Keycloak, etc.), logrando la suplantación de la aplicación y el acceso a APIs e información confidencial con todos los privilegios asignados.

Recomendaciones de mitigación:

1. Actualización prioritaria del SDK de Python: Desplegar inmediatamente la actualización del paquete mcp a las versiones 1.30.0 (rama 1.x) o 2.2.0 (rama 2.x) o superiores para restituir la validación estricta de metadatos OAuth.
2. Configuración obligatoria del emisor explícito (issuer=): Configurar explícitamente el parámetro issuer= con la URL exacta del servidor de autenticación en todas las instanciaciones de ClientCredentialsOAuthProvider y PrivateKeyJWTAuthProvider para impedir el seguimiento de servidores arbitrarios.
3. Depuración de registros OAuth almacenados y migración de proveedores obsoletos: Eliminar las registraciones dinámicas de clientes guardadas localmente antes de la versión corregida para forzar su recreación vinculada al emisor, y migrar las integraciones que utilicen la clase obsoleta RFC7523OAuthClientProvider.
4. Rotación de secretos y revocación de tokens de acceso: Realizar la rotación inmediata de los secretos de cliente (client_secrets) y revocar los tokens de acceso activos en el proveedor de identidad para cualquier cliente que haya interactuado con servidores MCP externos o no de confianza.

Prioridad: Crítica.

Ampliar información:

- <https://insylux.co/mcp-python-oauth-credenciales-colombia/>
- <https://forkast.news/anthropics-official-mcp-python-sdk-had-an-oauth-credential-stealing-flaw-that-let-any-malicious-server-hijack-your-login/>
- <https://aviatrix.ai/threat-research-center/mcp-python-sdk-oauth-credential-theft-2026/>
- <https://skycloak.io/blog/mcp-python-sdk-oauth-credential-theft-keycloak-issuer-pinning/>
- <https://tech.yahoo.com/ai/claude/articles/anthropic-official-mcp-python-sdk-071851694.html>

TEAMVIEWER – VULNERABILIDAD ALTA DE CONTROL DE ACCESO PERMITE EVADIR RESTRICCIONES DE SESIÓN Y EJECUTAR CÓDIGO REMOTO (CVE-2026-92370)

TeamViewer ha publicado un boletín de seguridad (TV-2026-1010) para corregir una vulnerabilidad de severidad alta de control de acceso en las aplicaciones TeamViewer Full Client y Host. La falla permite a un atacante remoto autenticado modificar los parámetros de control de acceso durante la fase de establecimiento de la sesión remota para evadir las restricciones de permisos configuradas por el usuario de destino. Esta evasión permite invocar funcionalidades explícitamente denegadas y ejecutar acciones no autorizadas, pudiendo derivar en la ejecución remota de código (RCE).

Resumen técnico:

- Identificador principal: CVE-2026-92370.
- Severidad: Alta (CVSS v3.1: 8.8 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).
- Causa raíz: Control de acceso inadecuado en el establecimiento y negociación de parámetros de sesiones remotas (CWE-284).
- Mecanismo de falla:
- Durante el proceso de establecimiento de una sesión remota, el cliente y el host negocian los permisos y las capacidades permitidas dentro del canal.
- Un atacante remoto previamente autenticado en la plataforma puede interceptar o manipular los paquetes de solicitud de sesión para alterar los parámetros de control de acceso antes de que el usuario objetivo aplique sus políticas locales.
- La aplicación falla en validar de forma estricta el cumplimiento de la configuración establecida por la víctima, permitiendo al atacante habilitar funciones restringidas o denegadas.
- Una vez omitidos los controles de permiso, el atacante invoca comandos o funciones privilegiadas dentro del contexto del proceso de TeamViewer, lo que habilita la ejecución de acciones arbitrarias e incluso la ejecución remota de código en el sistema cliente o Host.
- Estado de explotación: Divulgada oficialmente por TeamViewer el 29 de septiembre de 2026 (corregida en la versión 15.82 y compilaciones de mantenimiento específicas). No se registra evidencia de explotación activa en el entorno real ni disponibilidad de exploit público al momento de la publicación.
- Versiones afectadas: TeamViewer Full Client y Host en versiones anteriores a la 15.82 para Windows, Linux y macOS. También afecta a las ramas de mantenimiento y legacy: v15.64 (< 15.64.8 en Windows 7/8), v14.7 (< 14.7.48855 en Windows, Linux, macOS) y v13.2 (< 13.2.36230 en Windows, < 13.2.153995 en Linux, < 13.2.153994 en macOS).

Impacto potencial:

- Evasión directa de las políticas de seguridad de sesión: Permite a un usuario remoto autenticado anular las restricciones locales configuradas para bloquear transferencia de archivos, control interactivo o ejecución de scripts.
- Ejecución remota de código (RCE) no autorizada: Otorga la capacidad de ejecutar comandos arbitrarios en el sistema operativo del equipo objetivo con los privilegios asignados al proceso de TeamViewer.
- Acceso y exfiltración de información confidencial: Facilita la interacción no deseada con la interfaz gráfica, el sistema de archivos y las aplicaciones en ejecución en la máquina de la víctima.
- Punto de apoyo para movimiento lateral en la red: El compromiso de agentes TeamViewer Host (especialmente en servidores o estaciones con acceso desatendido) habilita al atacante a pivotar e infectar otros activos internos de la organización.

Recomendaciones de mitigación:

1. Actualización prioritaria del software: Desplegar inmediatamente la versión 15.82 o superior de TeamViewer Full Client y Host en todos los sistemas Windows, Linux y macOS, o sus versiones de mantenimiento parcheadas (15.64.8, 14.7.48855, 13.2.36230, etc.).
2. Restricción y auditoría de accesos desatendidos: Auditar las configuraciones de acceso no presencial (unattended access) y limitar la lista de usuarios y dispositivos autorizados a establecer conexiones entrantes.
3. Eliminación de instancias no esenciales de TeamViewer: Identificar y desinstalar agentes o clientes de TeamViewer en servidores críticos, estaciones administrativas o endpoints donde la herramienta no sea estrictamente necesaria.
4. Monitoreo de tráfico y segmentación de red: Restringir el tráfico de sesiones remotas mediante firewalls corporativos y monitorear los registros de eventos de TeamViewer para detectar sesiones con comportamientos o parámetros anómalos.

Prioridad: Crítica.

Ampliar información:

- <https://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2026-1010/?>
- <https://aviatrix.ai/threat-research-center/teamviewer-severe-flaws-patch-cve-2026-92370/>
- <https://www.truesec.com/hub/blog/multiple-high-severity-vulnerabilities-in-teamviewer>
- <https://radar.offsec.com/threat/an-improper-access-control-vulnerability-in-teamviewer-full-client-host-and-related-affected-modules-1cf7471488c0da5e>
- <https://mallory.ai/vulnerabilities/CVE-2026-92370>

OPENSSL – VULNERABILIDAD ALTA DE LECTURA FUERA DE LÍMITES EN RETRANSMISIONES DTLS PERMITE FILTRACIÓN DE MEMORIA DEL HEAP Y DENEGACIÓN DE SERVICIO (CVE-2026-84782)

El Proyecto OpenSSL ha publicado actualizaciones de seguridad de severidad alta para corregir una vulnerabilidad de lectura fuera de límites (CWE-125) en la lógica de retransmisión del protocolo Datagram Transport Layer Security (DTLS). La falla ocurre cuando la retransmisión de un mensaje de saludo (handshake) expirado se ejecuta mientras otra operación de escritura se encuentra suspendida (WANT_WRITE). Esta condición provoca que OpenSSL reutilice el búfer interno sin reiniciar el puntero de lectura, enviando datos adyacentes de la memoria dinámica (heap) en texto plano hacia el par conectado o provocando la caída abrupta del proceso (crash) cuando la lectura alcanza regiones de memoria no mapeadas.

Resumen técnico:

- Identificador principal: CVE-2026-84782.
- Severidad: Alta (CVSS v3.1: 8.2 en cve.org / 7.4 en Red Hat. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H).
- Causa raíz: Lectura fuera de límites (CWE-125) debido al manejo inadecuado del estado y puntero de lectura en la lógica de retransmisión de mensajes DTLS en entornos de E/S no bloqueante.
- Mecanismo de falla:
- En el protocolo DTLS sobre UDP, los mensajes de saludo pueden fragmentarse y retransmitirse. Si el transporte no puede aceptar más datos temporalmente, la escritura del mensaje se suspende devolviendo el estado WANT_WRITE.
- Mientras esa escritura permanece en pausa, el temporizador de retransmisión de DTLS se activa de forma independiente para retransmitir un mensaje enviado previamente desde la cola de retransmisión.
- Las versiones vulnerables de la biblioteca reutilizaban el mismo búfer interno y control de posición que el mensaje suspendido, sin restablecer el desplazamiento de lectura al inicio del mensaje que se iba a retransmitir.
- Esto provocaba que la retransmisión comenzara en una posición obsoleta, adjuntando bytes sobrantes y leyendo más allá del búfer asignado hacia la memoria heap adyacente, la cual se transmitía como datos de saludo no cifrados. Si la lectura alcanzaba memoria no asignada, el proceso colapsaba inmediatamente.
- Estado de explotación: Divulgada oficialmente el 29 de septiembre de 2026 (corregida en las versiones 4.0.3, 3.6.5, 3.5.9 y 3.4.8). No se registra evidencia de explotación activa en el entorno real al momento de la publicación.
- Versiones afectadas: OpenSSL en versiones de las ramas 4.0 (< 4.0.3), 3.6 (< 3.6.5), 3.5 (< 3.5.9), 3.4 (< 3.4.8), 3.0 (< 3.0.23, soporte premium), 1.1.1 (< 1.1.1zj, soporte premium) y 1.0.2 (< 1.0.2zs, soporte premium).

Impacto potencial:

- Filtración y exposición de memoria confidencial del servidor (heap): Permite a un atacante remoto obtener contenidos adyacentes del proceso transmitidos como texto plano en la sesión de saludo DTLS.
- Denegación de Servicio (DoS) por caída del proceso: Provoca el colapso (crash) o terminación inesperada del servicio web/servidor cuando la lectura fuera de límites intenta acceder a regiones de memoria no mapeadas.
- Inconsistencia de estado y corrupción del socket de comunicación: Invalida el seguimiento compartido de operaciones suspendidas, causando fallos en llamadas posteriores como SSL_read(), SSL_write(), SSL_accept() o SSL_connect().
- Afectación en infraestructura y servicios basados en UDP/DTLS: Expone a riesgo a servicios de telefonía e internet (VoIP), plataformas de video/audio en tiempo real (WebRTC), soluciones de acceso remoto VPN y dispositivos IoT/embebidos.

Recomendaciones de mitigación:

1. Actualización prioritaria de las librerías OpenSSL: Actualizar inmediatamente a las versiones corregidas de las ramas públicas mantenidas 4.0.3, 3.6.5, 3.5.9 o 3.4.8 (o solicitar 3.0.23, 1.1.1zj o 1.0.2zs para contratos de soporte premium).
2. Inventariar dependencias y binarios empaquetados: Realizar un escaneo completo en el sistema operativo y en aplicaciones que empaqueten internamente copias estáticas o dinámicas de OpenSSL, las cuales no suelen detectarse mediante los gestores de paquetes tradicionales.
3. Despliegue de parches en distribuidores de SO: Aplicar de forma urgente los paquetes de seguridad emitidos por la distribución del sistema operativo (por ejemplo, los paquetes libssl3t64 / libssl3 en Ubuntu o Debian).
4. Reiniciar servicios y aplicaciones afectadas: Ejecutar un reinicio completo de los servicios, daemons y soluciones VPN que utilicen OpenSSL DTLS para garantizar que las nuevas librerías en disco sean cargadas correctamente en memoria.

Prioridad: Crítica.

Ampliar información:

- <https://blog.elhacker.net/2026/09/openssl-corrige-fallo-grave-que-filtra.html>
- <https://ubuntu.com/security/notices/USN-8847-1>
- <https://thehackernews.com/2026/09/openssl-fixes-high-severity-dtls-flaw.html>
- <https://access.redhat.com/security/cve/cve-2026-84782>
- <https://csirt.telconet.net/comunicacion/boletines-servicios/openssl-corrige-vulnerabilidad-de-exposicion-de-memoria-en-dtls/>

MALWARE

MALWARE — SECTOPRAT / ARECHCLIENT2: NUEVA VARIANTE DE TROYANO DE ACCESO REMOTO OCULTA EN SOFTWARE LEGÍTIMO Y DISTRIBUIDA VÍA INGENIERÍA SOCIAL PERMITE CONTROL TOTAL Y ROBO DE INFORMACIÓN

Investigadores de ciberseguridad de FortiGuard Labs (Fortinet) y Huntress han documentado la aparición y evolución de nuevas campañas del troyano de acceso remoto (RAT) e infostealer SectopRAT (también conocido como ArechClient2). Desarrollado sobre la plataforma .NET y fuertemente ofuscado, el malware ha sido detectado oculto dentro de software legítimo de Windows mediante la manipulación de DLLs (DLL sideloading), así como distribuido mediante señuelos de ingeniería social ClickFix apoyados en falsos Custom GPTs de ChatGPT. La amenaza cuenta con 29 comandos de control remoto que permiten ejecutar órdenes administrativas, capturar pantallas, manipular archivos y extraer credenciales de navegadores, clientes de correo y billeteras de criptomonedas.

Resumen técnico:

- Identificador principal: SectopRAT / ArechClient2 (variantes investigadas en septiembre de 2026).
- Tipo de amenaza: Troyano de Acceso Remoto (Remote Access Trojan - RAT) / Infostealer / Cargador de Malware (Loader).
- Mecanismo de acceso e infección:
- Infección vía manipulación de software (DLL Sideload): Los atacantes alteran la tabla de importación de archivos de soporte legítimos (como FrameworkBase.dll) en aplicaciones en C:\ProgramData para forzar la carga de un módulo malicioso (sdkcra.dll). Este componente descifra shellcode y el payload de SectopRAT ocultos dentro de archivos de base de datos (Activation.Desktop.db y pool.db), ejecutándose de forma automática mediante tareas programadas de Windows.
- Infección vía ingeniería social (ClickFix y Custom GPTs): Los atacantes crean falsos modelos en ChatGPT (como "Plus 5.6") y anuncios maliciosos que redirigen hacia sitios en Google Sites disfrazados de verificaciones CAPTCHA de Cloudflare. Mediante engaños ClickFix, el usuario es inducido a ejecutar comandos en PowerShell que descargan un instalador MSI, el cual abusa de aplicaciones firmadas legítimas (de fabricantes como Canon o Stardock) para realizar DLL sideloading del malware.
- Capacidades operativas y canal de Comando y Control (C2):
- Control remoto y ejecución: Soporta 29 comandos remotos cifrados con AES que permiten tomar capturas de pantalla, abrir consolas interactivas (CMD/PowerShell), gestionar el sistema de archivos y procesos, reiniciar el equipo y ejecutar comandos de autodesinstalación.
- Módulo de robo de información (WbElevation.dll): Descarga módulos secundarios para extraer contraseñas, historial de autocompletado, cookies y datos de tarjetas de crédito almacenados en más de 40 navegadores web (Chrome, Edge, Firefox, Brave, etc.), clientes de correo (Thunderbird), aplicaciones de juego (Steam, Battle.net) y billeteras de criptomonedas (MetaMask, Atomic Wallet, Exodus, Electrum).

- Canal C2 y evasión: Mantiene comunicaciones cifradas con servidores de mando primarios y utiliza 12 endpoints de respaldo alojados en la red de Binance Coin (BNB) o consultas DNS sobre HTTPS (DoH) mediante resolvers públicos (Cloudflare, Google, Quad9) para evadir bloqueos por firmas de red y listas negras de IP.
- Estado de actividad: Campaña activa identificada a finales de septiembre de 2026, afectando a usuarios y sistemas empresariales basados en Windows.
- Plataformas afectadas: Sistemas operativos Microsoft Windows (arquitecturas de 32 y 64 bits).

Impacto potencial:

- Control remoto total y ejecución arbitraria de comandos: Otorga a los atacantes una consola interactiva completa (CMD/PowerShell) para explorar el sistema de archivos, gestionar procesos y ejecutar acciones con los privilegios del usuario comprometido.
- Compromiso y exfiltración masiva de credenciales y activos criptográficos: Permite el robo sistemático de contraseñas guardadas en navegadores, cookies de sesión, registros de autocompletado y claves de acceso a billeteras digitales de criptomonedas.
- Despliegue de cargas maliciosas secundarias y persistencia: Funciona como un cargador (dropper) capaz de descargar e instalar otros malware (como ransomware o infostealers) y establecer persistencia doble mediante claves de registro Run y tareas programadas.
- Evasión de defensas y alta resiliencia de la infraestructura: El uso de ejecutables firmados legítimos, ofuscación de código .NET, evasión de AMSI (Antimalware Scan Interface) y resolución C2 alternativa dificulta su detección por soluciones antivirus tradicionales.

Recomendaciones de mitigación:

1. Monitoreo y detección de DLL Sideloadin: Configurar reglas en soluciones EDR para detectar la ejecución de binarios legítimos o firmados lanzados desde rutas inusuales de perfil de usuario (AppData\Local, ProgramData) que carguen librerías DLL no firmadas o modificadas.
2. Auditoría e inspección de comandos en consola: Implementar políticas de restricción de ejecución en PowerShell y supervisar invocaciones de comandos sospechosas originadas desde la ventana Ejecutar de Windows (Win+R) o consolas lanzadas desde el navegador web.
3. Supervisión de tareas programadas y registro de inicio automático: Auditar de forma periódica la creación de tareas programadas y modificaciones en la clave del Registro HKCU\Software\Microsoft\Windows\CurrentVersion\Run iniciadas por cuentas de usuario.
4. Capacitación contra ingeniería social y filtrado de navegación: Concientizar al personal sobre los riesgos de copiar y pegar comandos indicados en ventanas emergentes o falsos CAPTCHAs (técnica ClickFix) y bloquear dominios/IPs asociados a la infraestructura de la amenaza.

Prioridad: Urgente.

Ampliar información:

- <https://www.fortinet.com/blog/threat-research/uncovering-a-sectopratt-variant-embedded-in-legitimate-software>
- <https://www.darkreading.com/cyberattacks-data-breaches/sectopratt-returns-hiding-inside-legitimate-application>
- <https://malwaretips.com/blogs/sectopratt-tampered-audio-software-fortinet/>
- https://cybersecuritynews.com/fortinet-uncovers-sectopratt/#google_vignette
- <https://www.huntress.com/blog/chatgpt-custom-gpts-clickfix-rat>

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

CITRIX NETSCALER (ADC Y GATEWAY) – EXPLOTACIÓN ACTIVA DE DOS VULNERABILIDADES CRÍTICAS ZERO-DAY PERMITE EJECUCIÓN REMOTA DE CÓDIGO Y DESPLIEGUE DE WEB SHELLS (CVE-2026-88771 Y CVE-2026-88772)

Citrix y diversos centros de inteligencia de amenazas (incluyendo CISA y agencias internacionales de ciberseguridad) han advertido sobre la explotación activa en el entorno real de dos vulnerabilidades zero-day de severidad crítica en Citrix NetScaler ADC y NetScaler Gateway. Los fallos permiten a atacantes remotos no autenticados ejecutar código arbitrario (RCE), instalar web shells camufladas y desplegar herramientas de tunelización para vulnerar la red interna corporativa. Debido a la gravedad y a la telemetría de explotación real, la agencia CISA incorporó ambos identificadores a su catálogo KEV exigiendo su mitigación obligatoria antes del 30 de septiembre de 2026.

Resumen técnico:

- Identificadores principales: CVE-2026-88771 y CVE-2026-88772.
- Severidad: Crítica (CVSS v4.0: 9.5).
- Causa raíz: Validación de entrada incorrecta (CWE-20) en CVE-2026-88771 y desbordamiento de memoria (buffer overflow) en la lógica DTLS (CWE-120) en CVE-2026-88772.
- Mecanismo de falla:
- CVE-2026-88771: Afecta a despliegues de NetScaler ADC y Gateway con la configuración predeterminada sin requerir autenticación ni requisitos especiales, permitiendo la inyección de comandos en el sistema.
- CVE-2026-88772: Se activa en entornos con el protocolo DTLS habilitado (opción activa por defecto en los VPN vServers), donde el desbordamiento de memoria conduce a la ejecución remota de código o a la caída del servicio.
- Persistencia y evasión avanzada: Los atacantes alteran la configuración del servidor web (httpd.conf) mediante reglas Alias o AliasMatch para procesar archivos con extensiones inofensivas (como .css o imágenes) como código PHP ejecutable, alojando web shells cifradas (como WHIPSHOT).
- Escalación de privilegios y tunelización: Los intrusos activan el bit setuid en /bin/sh para ejecutar comandos con privilegios de root y despliegan herramientas de tunelización TCP en Python (como SLAPSHOT) para pivotar hacia la red interna.
- Estado de actividad: Confirmada la explotación activa masiva a nivel global a finales de septiembre de 2026. CISA fijó el 30 de septiembre de 2026 como fecha límite de remediación para agencias federales.
- Versiones afectadas: Citrix NetScaler ADC y NetScaler Gateway en versiones 13.1 (anteriores a 13.1-64.23) y 14.1 (anteriores a 14.1-73.37), incluyendo compilaciones FIPS y NDcPP. Las versiones en fin de vida (EoL) 12.1 y 13.0 resultan vulnerables y no recibirán parches.

Impacto potencial:

- Ejecución remota de código (RCE) sin autenticación: Permite a un atacante no autenticado tomar control absoluto del dispositivo perimetral expuesto con máximos privilegios del sistema (root).
- Implantación de persistencia sigilosa e indetectable: Habilita la instalación de web shells PHP modificando el comportamiento del servidor web (httpd.conf) y elevando privilegios locales mediante la manipulación del binario /bin/sh.
- Movimiento lateral y pivotaje hacia la red interna: Facilita el despliegue de herramientas de tunelización TCP (como SLAPSHOT) para evadir la segmentación perimetral y acceder a servidores internos, bases de datos y controladores de dominio.

Compromiso total de la infraestructura VPN y acceso remoto: Expone el canal de entrada principal de la organización, permitiendo la interceptación de credenciales

Recomendaciones para mitigar el riesgo:

1. Actualización prioritaria a versiones soportadas corregidas: Actualizar de inmediato los appliances a las versiones 14.1-73.37 o 13.1-64.23 (o superiores) y planificar la migración obligatoria para instancias en versiones discontinuadas (12.1 y 13.0).
2. Evaluación de compromiso e inspección forense previa: Realizar una auditoría de seguridad antes de aplicar el parche para no sobrescribir evidencias, revisando permisos anómalos en /bin/sh, archivos en /var/netcaler/logon/LogonPoint/custom/ y directivas extrañas en httpd.conf.
3. Aplicación de mitigaciones temporales en red: En caso de no poder actualizar inmediatamente, deshabilitar la funcionalidad DTLS en los vServers de VPN y bloquear el tráfico UDP entrante al puerto 443 en el firewall perimetral para atenuar la vía de ataque de CVE-2026-88772.
4. Caza de amenazas (Threat Hunting) y monitoreo de procesos: Inspeccionar ejecuciones inusuales de procesos Python (lanzados con nohup), la presencia de archivos temporales como /tmp/.uxdport o /tmp/.uxdlock y patrones de tráfico de tunelización saliente desde el appliance.

Prioridad: Urgente.

Ampliar Información:

- <https://unaaldia.hispasec.com/una-campana-explota-dos-zero-days-criticos-en-citrix-netscaler-para-instalar-web-shells-y-moverse-por-la-red/>
- <https://korben.info/es/citrix-netscaler-otra-vez-a-parchear.html>
- <https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>
- <https://aviatrix.ai/threat-research-center/citrix-netscaler-saml-zero-day-cve-2026-88779-exploited-attacks/>
- <https://blog.elhacker.net/2026/10/nueva-vulnerabilidad-de-dia-cero-en.html>