Una vulnerabilidad en la implementación del protocolo HTTP/2 de NGINX podría permitir que un atacante ejecute código en servidores que tengan habilitada esta funcionalidad, sin necesidad de autenticarse previamente.

La falla, que tiene aproximadamente diez años de antigüedad, fue identificada como CVE-2026-123007 y recibió el nombre de «nginx2root». Este problema ha estado presente en el código de código abierto de NGINX desde la versión 1.9.5, publicada el 22 de septiembre de 2015. Las versiones que corrigen esta vulnerabilidad, 1.31.9 y 1.30.7, fueron lanzadas el día de hoy.

F5, empresa responsable del desarrollo de NGINX, explicó que los atacantes pueden ejecutar código en sistemas donde ASLR (Address Space Layout Randomization) se encuentre desactivado o sea posible evadirlo. Por su parte, especialistas en seguridad de Wiz afirmaron que consiguieron superar esta protección y ejecutar código mediante la vulnerabilidad durante sus pruebas. Los investigadores de Xint también demostraron la ejecución de código, utilizando únicamente un puerto HTTP/2 accesible.

El código ejecutado mediante este procedimiento adquiere los permisos correspondientes al proceso worker de NGINX. Sin embargo, obtener privilegios de administrador (root) en el sistema anfitrión requiere recurrir a un mecanismo adicional de escalamiento de privilegios, según informó CIRCL (Computer Incident Response Center Luxembourg).

Durante las pruebas realizadas por Xint, los investigadores comprobaron que un código ejecutado con los permisos de un proceso worker podía alcanzar privilegios root en el sistema anfitrión mediante otra vulnerabilidad independiente localizada en el código SCTP del kernel de Linux. Este comportamiento también se presentó cuando NGINX se ejecutaba dentro de un contenedor Docker.

Hasta el momento, ni el fabricante ni los investigadores de Wiz y Rapid7 han comunicado la existencia de ataques reales que aprovechen esta vulnerabilidad. Asimismo, al día de hoy, la falla todavía no aparecía en el catálogo de vulnerabilidades explotadas conocidas (Known Exploited Vulnerabilities) de CISA.

En GitHub se encuentra disponible públicamente un código de prueba de concepto (PoC) relacionado con esta falla. No obstante, las indicaciones que acompañan al código especifican que únicamente permite demostrar el ataque contra un contenedor Docker recién iniciado en la misma máquina.

De acuerdo con los avisos de seguridad publicados por NGINX, todas las versiones de código abierto comprendidas entre la 1.9.5 y la 1.31.8 presentan esta vulnerabilidad. Esto incluye la versión 1.31.8, publicada el 21 de octubre, así como las actualizaciones de seguridad 1.31.7 y 1.30.6, distribuidas el 14 de octubre.

El producto NGINX Plus también se encuentra afectado. Según el comunicado del fabricante, el problema está presente en las versiones de la rama 37.x anteriores a las compilaciones corregidas, así como en las versiones R34 a R36.

Las actualizaciones publicadas hoy también solucionan otras cuatro vulnerabilidades que, bajo las mismas condiciones relacionadas con ASLR, podrían facilitar la ejecución de código. El fabricante asignó a las cinco fallas una puntuación de 9.2 sobre 10 en la escala CVSS 4.0.

Cada una de estas vulnerabilidades requiere condiciones específicas para poder ser aprovechada:

Vulnerabilidad	Condiciones necesarias para su explotación
CVE-2026-123007	Tener habilitado el protocolo HTTP/2.
CVE-2026-123633	Contar con HTTP/2 habilitado y reenviar solicitudes a un servidor backend mientras el proceso worker dispone de una cantidad reducida de conexiones worker_connections.
CVE-2026-123634	Utilizar un nombre de servidor proxy construido mediante variables, junto con una directiva de inclusión del lado del servidor (SSI) o una solicitud secundaria mirror hacia una ubicación que intente resolver ese mismo nombre.
CVE-2026-121810	Tener habilitado el protocolo HTTP/3.
CVE-2026-113425	Utilizar NGINX como servidor proxy de correo electrónico.

El protocolo HTTP/2 se encuentra habilitado cuando una directiva listen incorpora el parámetro http2 o cuando se establece la configuración http2 on. Para comprobar si un servidor admite este protocolo, es posible ejecutar el comando openssl s_client con el parámetro -alpn h2 contra el servicio correspondiente. Si la conexión acepta HTTP/2, la salida mostrará el mensaje ALPN protocol: h2.

Cuando el servidor se encuentra detrás de una CDN, la comprobación debe realizarse directamente contra el servidor de origen de NGINX. Esto se debe a que, si el servidor de origen únicamente admite HTTP/1.1, no será posible aprovechar la vulnerabilidad mediante HTTP/2 a través de esa conexión.

Correcciones, medidas de mitigación e indicadores de posibles ataques

De acuerdo con F5, las siguientes versiones incorporan las correcciones correspondientes a CVE-2026-123007:

- NGINX Open Source 1.31.0 a 1.31.8 (rama principal): la corrección está disponible en la versión 1.31.9.
- NGINX Open Source 1.9.5 a 1.30.6, incluidas ramas anteriores como la 1.28: la solución se incorporó en la versión 1.30.7.
- NGINX Plus 37.1.0 a 37.2.0.1: corregido en la versión 37.3.0.1.
- NGINX Plus 37.0.0 a 37.0.7.1: corregido en la versión 37.0.8.1.
- NGINX Plus R34 a R36: el fabricante no señala una actualización correctiva para estas versiones.

Según las notas oficiales de lanzamiento de NGINX, las versiones 1.31.9 y 1.30.7 solucionan las cinco vulnerabilidades identificadas. En el caso de NGINX Plus, las versiones 37.3.0.1 y 37.0.8.1 corrigen cuatro de ellas, mientras que la solución para CVE-2026-123633 ya se había incorporado en las compilaciones anteriores 37.2.0.1 y 37.0.7.1.

Una vez instalada la actualización, es necesario reiniciar completamente NGINX o realizar una actualización del ejecutable en caliente (*live binary upgrade*). Una simple recarga de la

configuración no es suficiente, ya que el proceso podría continuar utilizando el ejecutable anterior y mantener conexiones existentes asociadas con procesos worker que todavía no han sido actualizados.

Las imágenes oficiales de Docker de NGINX ya contaban, al día de hoy, con las etiquetas correspondientes a las versiones 1.31.9 y 1.30.7, incluidas sus variantes basadas en Alpine.

Por otro lado, Ubuntu y Debian todavía no habían distribuido paquetes con las correcciones correspondientes. La página de seguimiento de CVE de Ubuntu identificaba el paquete nginx como vulnerable en sus versiones comprendidas entre 16.04 y 26.10. De manera similar, el rastreador de seguridad de Debian mantenía la condición de vulnerable para las ramas bookworm, trixie, forky y sid.

Es importante considerar que los paquetes proporcionados por una distribución pueden incorporar una solución de seguridad sin modificar el número de versión que muestra el comando nginx -v. Por este motivo, se recomienda verificar la versión completa del paquete e identificar si corresponde a una actualización reconocida en los avisos oficiales de seguridad de cada distribución.

El fabricante únicamente documentó medidas alternativas de protección para dos de las cinco vulnerabilidades. En el caso de la falla relacionada con el resolver, identificada como CVE-2026-123634, se recomienda evitar el uso de las directivas SSI y mirror, además de no construir nombres de servidores proxy mediante variables.

Respecto a la vulnerabilidad que afecta al proxy de correo, CVE-2026-113425, la recomendación consiste en restringir los puntos de escucha del servicio para que únicamente sean accesibles desde redes consideradas confiables.

Las recomendaciones de respuesta a incidentes de CIRCL incluyen deshabilitar temporalmente HTTP/2 como medida de protección mientras se prepara la actualización del software. Esta acción permite bloquear las condiciones de explotación de CVE-2026-123007 y CVE-2026-123633, aunque no proporciona protección frente a las otras tres vulnerabilidades.

Asimismo, desactivar HTTP/3 en los entornos donde esté habilitado elimina las condiciones necesarias para aprovechar CVE-2026-121810.

En las versiones de NGINX 1.25.1 y posteriores, es necesario establecer el parámetro http2 off; dentro de cada bloque de servidor afectado y retirar http2 de las directivas listen correspondientes.

Para las versiones comprendidas entre la 1.9.5 y la 1.25.0, basta con eliminar el parámetro http2 de la directiva listen. Por ejemplo, la configuración listen 443 ssl http2; debe modificarse para quedar como listen 443 ssl;.

Después de realizar estos cambios, se debe reiniciar NGINX cuando corresponda y repetir la comprobación mediante OpenSSL para verificar que el servidor haya dejado de aceptar conexiones HTTP/2.

Mientras no se corrija la vulnerabilidad SCTP presente en el kernel de Linux, las recomendaciones también contemplan impedir la carga del módulo correspondiente en aquellos equipos que no utilicen SCTP, un protocolo de transporte de red similar a TCP.

Una de las alternativas consiste en incorporar la línea install sctp /bin/false en un archivo con extensión .conf ubicado dentro del directorio /etc/modprobe.d/. Sin embargo, esta medida no descarga un módulo que ya se encuentre activo ni deshabilita SCTP cuando está integrado directamente en el kernel.

En cuanto a la identificación de posibles actividades maliciosas, CIRCL recomienda prestar atención a diferentes comportamientos anómalos, entre ellos:

- Procesos worker de NGINX que inician programas o aplicaciones inesperadas.
- Procesos worker que finalizan de manera irregular o generan archivos de volcado de memoria (*core dumps*).
- Conexiones HTTP/2 de larga duración que reciben grandes cantidades de tráfico entrante, pero registran muy pocas solicitudes en los archivos de registro.

- Conexiones salientes inusuales o consultas DNS que no corresponden con el comportamiento habitual del servidor.

Es importante señalar que la ausencia de solicitudes sospechosas en los registros de acceso no descarta la posibilidad de un ataque. Esto ocurre porque los marcos de control de HTTP/2 normalmente no se registran como solicitudes convencionales. Además, ninguno de los indicadores mencionados constituye por sí solo una prueba concluyente de compromiso del sistema.

De acuerdo con el análisis técnico publicado por Rapid7, la variante de explotación desarrollada por sus investigadores requiere aproximadamente 128 GB de tráfico HTTP/2. Durante su demostración, el procedimiento de ataque se completó en alrededor de dos minutos y medio. Sin embargo, cuando se utilizan conexiones con velocidades inferiores a aproximadamente 300 Mbit/s, la transferencia puede superar el límite predeterminado de una hora establecido para las conexiones de NGINX, provocando que el ataque no consiga completarse.

El método de explotación también depende de una rutina de copia de memoria de glibc que se selecciona en procesadores x86-64 que incorporan las características avx512f y avx512vl.

Según la publicación de divulgación de Wiz, sus investigadores llevaron a cabo las pruebas utilizando compilaciones oficiales de NGINX 1.31.7 y 1.31.8, mediante conexiones HTTP/2 sobre TLS en sistemas de arquitectura de 64 bits.

Por último, el informe de investigación de Xint señala que su procedimiento de explotación funcionó contra servidores de prueba alojados en AWS, GCP y Azure, incluso cuando estos se encontraban expuestos mediante una dirección IP pública.