Alerta Vulnerabilidad
Vulnerabilidad crítica en NGINX

CSIRTSALUD-AV-20260519-47 **TLP: CLEAR**

Alerta ID:	47
Fecha del reporte:	19/05/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	CVE-2026-42945 — NGINX Rift
Herramienta de detección	N/A
Activo involucrado:	sistemas expuestos a internet
Tipo de alerta:	Alerta vulnerabilidad
Nivel de riesgo:	Alta

Resumen ejecutivo

Informar a las entidades sobre una vulnerabilidad crítica identificada en el servidor web NGINX, catalogada como CVE-2026-42945 y denominada NGINX Rift. Esta falla, con una antigüedad de 18 años desde su introducción en el código, se encuentra actualmente bajo explotación activa en entornos reales, lo que eleva significativamente el nivel de riesgo para las organizaciones del sector.

Descripción:

La vulnerabilidad CVE-2026-42945, denominada NGINX Rift, es un heap buffer overflow (desbordamiento de búfer en memoria dinámica) presente en el módulo ngx_http_rewrite_module de NGINX. Esta falla fue introducida en el código fuente en el año 2008 y permaneció sin detectarse durante aproximadamente 18 años.

Fue descubierta y divulgada responsablemente el 21 de abril de 2026 por la empresa de seguridad depthfirst, con la publicación de los parches el 14 de mayo de 2026. Apenas días después de su divulgación pública, el 17 de mayo de 2026, VulnCheck confirmó intentos de explotación activa contra sus redes de honeypot.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

La vulnerabilidad existe cuando en la configuración de NGINX se utiliza la directiva rewrite seguida de otra directiva rewrite, if o set, empleando capturas sin nombre de expresiones regulares compatibles con Perl (PCRE), como $1 o $2, junto con una cadena de reemplazo que contiene un signo de interrogación (?).

Un atacante remoto no autenticado puede enviar una solicitud HTTP especialmente crafteada que provoca un desbordamiento en el heap del proceso worker de NGINX. El resultado directo es el reinicio del worker (denegación de servicio), y en sistemas donde ASLR (Address Space Layout Randomization) está desactivado, es posible lograr ejecución remota de código (RCE).

Modo de explotación detallado.

- El servidor NGINX debe tener configurada la directiva rewrite con capturas sin nombre (p. ej., $1, $2) y un signo ? en la cadena de reemplazo.
- El servicio NGINX debe ser accesible desde la red del atacante (Internet o red interna).
- Para RCE: el sistema operativo debe tener ASLR desactivado (configuración no predeterminada en Linux moderno).
- Para DoS: no se requieren condiciones adicionales más allá de la configuración vulnerable.

Flujo de ataque paso a paso

1. Reconocimiento (TA0043): El atacante escanea Internet en busca de instancias NGINX vulnerables utilizando herramientas como Shodan, Censys, o versiones personalizadas de Vulnhuntr (herramienta de descubrimiento de vulnerabilidades asistida por IA). Identifica la versión de NGINX y posibles configuraciones de rewrite en respuestas HTTP.
2. Identificación de configuración vulnerable (TA0043/T1595): El atacante prueba patrones de URI específicos para determinar si el servidor tiene directivas rewrite con capturas sin nombre ($1, $2) seguidas de un signo ?. La respuesta del servidor (crash del worker vs respuesta normal) confirma la vulnerabilidad.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

3. Construcción de la solicitud maliciosa (TA0002): El atacante crafta una solicitud HTTP GET/POST con una URI especialmente diseñada que, al ser procesada por la directiva rewrite vulnerable, provoca que los bytes del URI del atacante se escriban más allá del límite de la asignación de memoria en el heap del proceso worker de NGINX.
4. Desbordamiento del heap (T1499.004): La URI maliciosa provoca que el módulo ngx_http_rewrite_module escriba datos controlados por el atacante fuera de los límites del buffer asignado en el heap. El proceso worker de NGINX cae y se reinicia automáticamente (DoS).
5. Escalada a RCE (si ASLR está desactivado) (T1203): En sistemas sin ASLR, el atacante puede predecir las direcciones de memoria y controlar el flujo de ejecución a través de los bytes escritos en el heap. Esto permite redirigir la ejecución a código arbitrario dentro del proceso worker de NGINX.
6. Post-explotación (TA0004/TA0008): Una vez con RCE, el atacante puede desplegar un webshell PHP para persistencia, ejecutar comandos del sistema, moverse lateralmente, robar credenciales o exfiltrar datos.

Indicadores de compromiso

A la fecha de publicación de este boletín, la actividad de explotación ha sido detectada principalmente desde infraestructura de origen chino según reportes de VulnCheck. A continuación, se listan los IOC observados y patrones de detección relevantes:

Tipo de IOC	Valor / Patrón	Descripción
Origen geográfico	IP de origen chino (TBD)	Actividad detectada por honeypot VulnCheck
User-Agent sospechoso	Posible Vulnhuntr customizado	Herramienta IA de descubrimiento de vulnerabilidades

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Tipo de IOC	Valor / Patrón	Descripción
Patrón URI	URI crafteada con ? en path de rewrite	Trigger del heap overflow
Artefacto en servidor	Webshell PHP (.php) en directorio web	Post-explotación observada en openDCIM
Comportamiento proceso	Nginx worker: restart loop	Worker NGINX en ciclo continuo de crash
Log HTTP	400/500 con URIs malformadas largas	Intentos de overflow en rewrite
Tráfico de red	Peticiones HTTP anómalas con query strings	Patrón de scanning/explotación

Vulnerabilidades.

En el mismo ciclo de divulgación, F5/NGINX corrigió cuatro vulnerabilidades en NGINX Plus y NGINX Open Source. A continuación se describe cada una:

CVE-2026-42945 — CRÍTICO (CVSS 9.2) — NGINX Rift

Módulo: ngx_http_rewrite_module | Tipo: Heap Buffer Overflow
Descripción: Heap buffer overflow que permite a un atacante remoto no autenticado enviar una solicitud HTTP crafteada para desbordar el heap del proceso worker de NGINX. En configuraciones con ASLR desactivado, permite RCE. En todas las configuraciones vulnerables,

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

permite DoS por reinicio del worker. Los bytes escritos fuera del buffer son controlados por el atacante a través de la URI, lo que hace la corrupción predecible y reproducible.
Condición: Requiere directiva rewrite con capturas sin nombre ($1, $2) + signo ? en cadena de reemplazo.

CVE-2026-42946 — ALTO (CVSS 8.3)

Módulo: ngx_http_scgi_module / ngx_http_uwsgi_module | Tipo: Asignación excesiva de memoria
Descripción: Vulnerabilidad de asignación excesiva de memoria que puede ser explotada por un atacante con capacidades de adversary-in-the-middle (AitM) que controle las respuestas de un servidor upstream. Permite leer la memoria del proceso worker de NGINX o provocar su reinicio. Activa cuando scgi_pass o uwsgi_pass están configurados.

CVE-2026-40701 — MEDIO (CVSS 6.3)

Módulo: ngx_http_ssl_module | Tipo: Use-After-Free
Descripción: Vulnerabilidad use-after-free que permite a un atacante remoto no autenticado con control limitado de modificación de datos reiniciar el proceso worker o modificar datos parcialmente. Se activa cuando ssl_verify_client está en 'on' u 'optional' y ssl_ocsp está en 'on'.

CVE-2026-42934 — MEDIO (CVSS 6.3)

Módulo: ngx_http_charset_module | Tipo: Lectura fuera de límites (Out-of-Bounds Read)
Descripción: Lectura fuera de límites que puede revelar el contenido de memoria del proceso worker o provocar su reinicio. Se activa cuando las directivas charset, source_charset, charset_map y proxy_pass con buffering desactivado ('off') están configuradas simultáneamente.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Principales activos afectados.

La siguiente tabla resume todos los productos y versiones afectadas por CVE-2026-42945, según el aviso oficial de F5 (K000161019):

Producto / Componente	Versiones Vulnerables	Versión con Parche
NGINX Open Source	0.6.27 – 1.30.0	1.30.1 / 1.31.0
NGINX Open Source (legacy)	0.6.27 – 0.9.7	**Sin parche planeado**
NGINX Plus	R32 – R36	R32 P6 / R36 P4
NGINX Instance Manager	2.16.0 – 2.21.1	Ver aviso F5
F5 WAF for NGINX	5.9.0 – 5.12.1	Ver aviso F5
NGINX App Protect WAF	4.9.0 – 4.16.0 / 5.1.0 – 5.8.0	Ver aviso F5
NGINX App Protect DoS	4.3.0 – 4.7.0	Ver aviso F5
F5 DoS for NGINX	4.8.0	Ver aviso F5
NGINX Gateway Fabric	1.3.0–1.6.2 / 2.0.0–2.5.1	Ver aviso F5
NGINX Ingress Controller	3.5.0–3.7.2 / 4.0.0–4.0.1 / 5.0.0–5.4.1	Ver aviso F5

Recomendaciones

- Monitorear los logs de NGINX (/var/log/nginx/error.log) en busca de mensajes de reinicio anómalo del worker, como: [alert] worker process NNNN exited on signal 11.
- Analizar logs de acceso HTTP en busca de solicitudes con URIs largas, caracteres especiales inusuales (especialmente ?) en rutas de rewrite, o patrones de scanning sistemático.
- Priorizar el parcheo de instancias NGINX expuestas directamente a Internet o que sirvan aplicaciones con datos de pacientes (PHI/PII).

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Validar que sistemas de seguridad perimetral (firewall, WAF, IPS) tengan reglas actualizadas para CVE-2026-42945.
- Mantener capacidad de respuesta a incidentes activada y escalar al CSIRT Salud ante cualquier indicador de compromiso confirmado.

Fuentes:

- The Hacker News. (17 mayo 2026). NGINX CVE-2026-42945 Exploited in the Wild, Causing Worker Crashes and Possible RCE. https://thehackernews.com/2026/05/nginx-cve-2026-42945-exploited-in-wild.html
- The Hacker News. (14 mayo 2026). 18-Year-Old NGINX Rewrite Module Flaw Enables Unauthenticated RCE. https://thehackernews.com/2026/05/18-year-old-nginx-rewrite-module-flaw.html
- F5 Networks. (2026). Security Advisory K000161019 — CVE-2026-42945. https://my.f5.com/manage/s/article/K000161019
- depthfirst Security. (2026). NGINX Rift — Technical Analysis. https://depthfirst.com/nginx-rift
- VulnCheck. (2026). CVE-2026-42945 Exploitation Activity. https://vulncheck.com
- AlmaLinux Maintainers. (13 mayo 2026). NGINX Rift CVE-2026-42945. https://almalinux.org/blog/2026-05-13-nginx-rift-cve-2026-42945/
- MITRE ATT&CK Framework v15. https://attack.mitre.org
- NVD NIST — CVE-2026-42945. https://nvd.nist.gov/vuln/detail/CVE-2026-42945
- CVE-2026-42946, CVE-2026-40701, CVE-2026-42934 — F5 Security Advisories K000161027, K000161021, K000161028.

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 3168931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570