Boletín de alerta

Boletín Nro.: 49
Fecha de publicación: 14/05/2026
Tema: Alerta 2026-49 Vulnerabilidad critica de mas de 18 años en NGINX
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

La vulnerabilidad afecta a:

- **NGINX Open Source**
  - Versiones desde **0.6.27 hasta 1.30.0** (incluidas).
- **NGINX Plus**
  - Versiones comerciales **R32 a R36**.

La vulnerabilidad se encuentra en el módulo **ngx_http_rewrite_module** y solo se manifiesta cuando se cumplen ciertas condiciones en las directivas **rewrite**, **if** o **set** que usan capturas PCRE sin nombre (**$1**, **$2**, etc.) con cadenas de reemplazo que contienen el carácter **?**.

Descripción

Recientemente se ha publicado una vulnerabilidad llamada **CVE 2026 42945 con un score CVSSv3.1 8.1**, apodada *"NGINX Rift"*, es un **heap buffer overflow** en el módulo ngx_http_rewrite_module de NGINX que puede ser explotado de forma remota mediante una única petición HTTP especialmente diseñada. Bajo configuración vulnerable, permite a un atacante no autenticado provocar **reinicios de los procesos worker** (Denial of Service), y en sistemas donde **ASLR está desactivado o debilitado**, puede abrir la puerta a **ejecución remota de código (RCE)**.

F5, como CNA de este CVE, evalúa el fallo con una severidad de **9.2 (CRITICAL) en CVSS v4.0** y 8.1 (High) en CVSS v3.1, y confirma que el bug lleva presente en el código desde 2008, afectando a todas las versiones de NGINX Open Source desde la 0.6.27. Dado que NGINX se usa masivamente como reverse proxy y front door de aplicaciones web y APIs, el impacto potencial para infraestructuras empresariales e ISPs es muy alto.

Condiciones para que exista la vulnerabilidad

El problema está en cómo **ngx_http_rewrite_module** gestiona determinadas reglas que combinan:

- Una directiva **rewrite, if o set** que utiliza **capturas PCRE sin nombre** ($1, $2, …)
- Una **cadena de reemplazo que incluye ?** (habitual cuando se reescriben rutas y query strings)
- Patrones donde ciertos caracteres como +, % y & pueden “expandirse” al re□escaparse, haciendo que la longitud resultante sea mayor que la calculada inicialmente.

En estas condiciones, el módulo calcula un tamaño de buffer insuficiente para el resultado, pero aun así escribe la cadena re□escapada, lo que provoca que la escritura se **desborde más allá del final del buffer** en el heap.

Vector de ataque

Un atacante remoto puede:

- Enviar **una única petición HTTP** cuidadosamente construida hacia un servidor NGINX que tenga reglas rewrite vulnerables.
- Forzar que se ejecute la ruta de código donde se produce el desbordamiento.
- Como mínimo, provocar que el worker de NGINX se caiga y se reinicie, generando un **DoS intermitente** o continuado.
- En entornos donde **ASLR está desactivado** (por ejemplo, sistemas legacy o configuraciones endurecidas manualmente pero mal testeadas), el contenido controlado que se escribe fuera del buffer puede permitir **RCE** si el atacante consigue una primitiva de corrupción útil.

Importante para sysadmins: el fallo no requiere autenticación, ni módulos “exóticos”: solo una configuración desafortunada del propio

A las pocas horas de publicarse el advisory, varios investigadores han liberado PoC públicos para CVE□2026□42945, incluyendo exploits funcionales en GitHub y write□ups técnicos detallando la cadena de explotación. Esto reduce drásticamente la ventana de tiempo entre la divulgación y la explotación masiva, por lo que se recomienda tratar esta vulnerabilidad como crítica y de explotación probable a muy corto plazo, priorizando la aplicación de parches y/o la reconfiguración de reglas rewrite vulnerables.

Mitigación

Mientras no se pueda aplicar actualización, F5 y varios vendors recomiendan las siguientes mitigaciones temporales:

1. **Revisar y corregir reglas rewrite vulnerables**
    - Auditar la configuración NGINX (nginx.conf y conf.d/*.conf) buscando directivas rewrite, if y set que:
        - usen capturas $1, $2, etc. y
        - incluyan ? en la cadena de reemplazo.
    - Reescribir estas reglas para evitar combinaciones que provoquen re□escapado “expandido” (por ejemplo, minimizando uso de +, %, & en patrones o cambiando la forma de construir la query string).
2. **Reducir superficie de exposición**

    - Limitar el acceso desde Internet solo a los endpoints necesarios (WAF, reverse proxies adicionales, VPN, etc.).
    - Usar listas de control de acceso (ACL) o firewalls para segmentar quién puede llegar a NGINX si se trata de paneles internos o APIs administrativas.
3. **Endurecer el sistema operativo**
    - Verificar que **ASLR esté habilitado** en todos los hosts que ejecutan NGINX; esto baja de forma significativa la probabilidad de explotación RCE, aunque no evita el DoS.
    - Asegurar que otras mitigaciones como stack canaries, RELRO y PIE estén activas según la distro.
4. **Monitorización y detección**
    - Activar logs de error y acceso y **monitorizar reinicios frecuentes** de procesos worker NGINX, especialmente en hosts expuestos a Internet.
    - Revisar herramientas EDR/NIDS para detectar patrones de request repetitivos hacia paths que disparan reglas rewrite complejas.

Solución:

La remediación definitiva pasa por **actualizar NGINX a versiones corregidas** según la guía de F5:

1. **NGINX Open Source**
    - Actualizar a una versión **posterior a 1.30.0** donde el bug ha sido corregido (por ejemplo, versiones 1.30.x o 1.31.x ya parcheadas según tu distribución).
    - En distros Linux, aplicar los paquetes de seguridad provistos por el vendor (AlmaLinux, Debian, Ubuntu, etc.) que ya incorporan el fix para CVE⊠2026⊠42945.
2. **NGINX Plus (F5)**
    - Actualizar a las versiones **R37 o superiores**, según el advisory K000161019 y la Quarterly Security Notification de mayo 2026.
    - Seguir la guía oficial de upgrade de F5 para NGINX Plus, validando compatibilidad con módulos comerciales y entorno (K000160932 y documentación de actualización de NGINX Plus).
3. **Plan de actualización recomendado**
    - Probar primero la actualización en un entorno de **pre producción** que replique las reglas rewrite y el tráfico típico.
    - Medir impacto en rendimiento y compatibilidad (módulos de terceros, WAF, Lua, etc.).
    - Programar ventana de mantenimiento para producción y aplicar la actualización siguiendo la guía de rollback (snapshot de VM, backup de configs).

En todos los casos, se recomienda documentar explícitamente que el riesgo asociado a CVE⊠2026⊠42945 queda mitigado solo cuando **se ha actualizado NGINX** y, en paralelo, se han revisado las reglas rewrite problemáticas.

Información adicional:

- F5 – **K000161019: NGINX ngx_http_rewrite_module vulnerability CVE?2026?42945**
- F5 – **K000160932: Quarterly Security Notification (May 2026)**

- NVD – **CVE?2026?42945**
- depthfirst – **NGINX Rift (CVE?2026?42945): An 18?Year?Old Heap Overflow**
- AlmaLinux – **NGINX Rift (CVE?2026?42945)**