

Boletín de alerta

Boletín Nro.: 116

Fecha de publicación: 19/10/2026

Tema: Alerta 2026-116 Vulnerabilidades críticas en NGINX permiten DoS servicio y RCE.

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

NGINX Open Source

CVE	Versiónes afectadas según nginx.org	Versiónes corregidas
CVE-2026-15176	0.1.29 a 1.31.6, salvo ramas que ya incorporen la corrección	1.30.6 en la rama estable o 1.31.7 en la rama principal, y posteriores
CVE-2026-93479	1.30.0 a 1.30.5 y 1.31.2 a 1.31.6	1.30.6 o 1.31.7, y posteriores
CVE-2026-97205	0.8.11 a 1.31.6, salvo ramas que ya incorporen la corrección	1.30.6 en la rama estable o 1.31.7 en la rama principal, y posteriores

NGINX Plus y productos integrados

Producto	Versiónes afectadas o alcance	Corrección publicada
NGINX Plus 37.x	37.0.0 a 37.0.4, para las tres CVE	37.0.5.1 o 37.1.0.1.
NGINX Plus R33-R36	Las ramas figuran como afectadas en los avisos	Sin corrección listada en esas ramas; consultar la ruta de actualización soportada.
F5 WAF for NGINX	Versiónes afectadas dentro del intervalo 5.9.0-5.15.0; el detalle varía por CVE	5.14.2 o 5.16.0, según la rama aplicable.
F5 DoS for NGINX	4.8.0 a 4.10.0	4.11.0.
NGINX Gateway Fabric	La afectación depende de la rama y de la CVE; los avisos incluyen 2.1.0-2.7.2	2.8.0 para la rama 2.x indicada.
NGINX Ingress Controller	Para CVE-2026-97205: 5.6.0 a 5.6.3	5.7.0. Validar por separado las demás CVE.

Descripción

Se publicaron tres vulnerabilidades de corrupción de memoria en NGINX: **CVE-2026-15176**, relacionada con el uso de *alias* y *rewrite*; **CVE-2026-93479**, asociada a la evaluación de variables y capturas de expresiones regulares; y **CVE-2026-97205**, vinculada al uso conjunto de SSI y operaciones de entrada/salida asíncronas —AIO—. Las tres tienen una puntuación CVSS v4.0 de 9.2 y pueden permitir que atacantes remotos sin autenticación provoquen la caída de procesos de trabajo. La ejecución de código es posible bajo condiciones adicionales, como ASLR deshabilitado o elusión de esa protección. La exposición depende de configuraciones específicas, no de la sola presencia de NGINX.

Vulnerabilidades y condiciones de exposición:

CVE	Descripción	Configuración que debe revisar el administrador
CVE-2026-15176	Desbordamiento de búfer en un proceso de trabajo al convertir una URI modificada en una ruta de archivo.	Uso de alias en un bloque location, cuando rewrite modifica la URI y esta se mapea posteriormente a una ruta; revisar también el uso de <code>\$request_filename</code> .
CVE-2026-93479	Desbordamiento de búfer al evaluar expresiones de texto con variables, con impacto en el cálculo de la raíz documental y el registro de solicitudes.	Directivas map con expresiones regulares cuyas variables de captura se utilizan en root o en el formato del registro de acceso antes de referenciar la variable de salida del map.
CVE-2026-97205	Uso de memoria después de liberarla — <i>use-after-free</i> — bajo determinadas configuraciones.	Uso conjunto de AIO y páginas SSI con instrucciones include virtual.

Solución

La solución consiste en actualizar NGINX Open Source a 1.30.6 o 1.31.7, o posteriores de la rama correspondiente, e instalar las versiones corregidas que F5 indique para NGINX Plus y los productos que lo integran.

Se debe priorizar a los servidores expuestos a Internet que utilicen las configuraciones vulnerables, verificar la versión realmente ejecutada después del cambio y completar la sustitución de procesos o contenedores antiguos.

Información adicional:

- F5 — CVE-2026-15176:
<https://my.f5.com/manage/s/article/K000162416f5>

- F5 — CVE-2026-93479:
<https://my.f5.com/manage/s/article/K000162607f5>
- F5 — CVE-2026-97205:
<https://my.f5.com/manage/s/article/K000162608f5>
- NGINX — avisos oficiales de seguridad:
https://nginx.org/en/security_advisories.htmlnginx
- BleepingComputer:
<https://www.bleepingcomputer.com/news/security/f5-releases-out-of-band-patches-for-critical-nginx-vulnerabilities/>