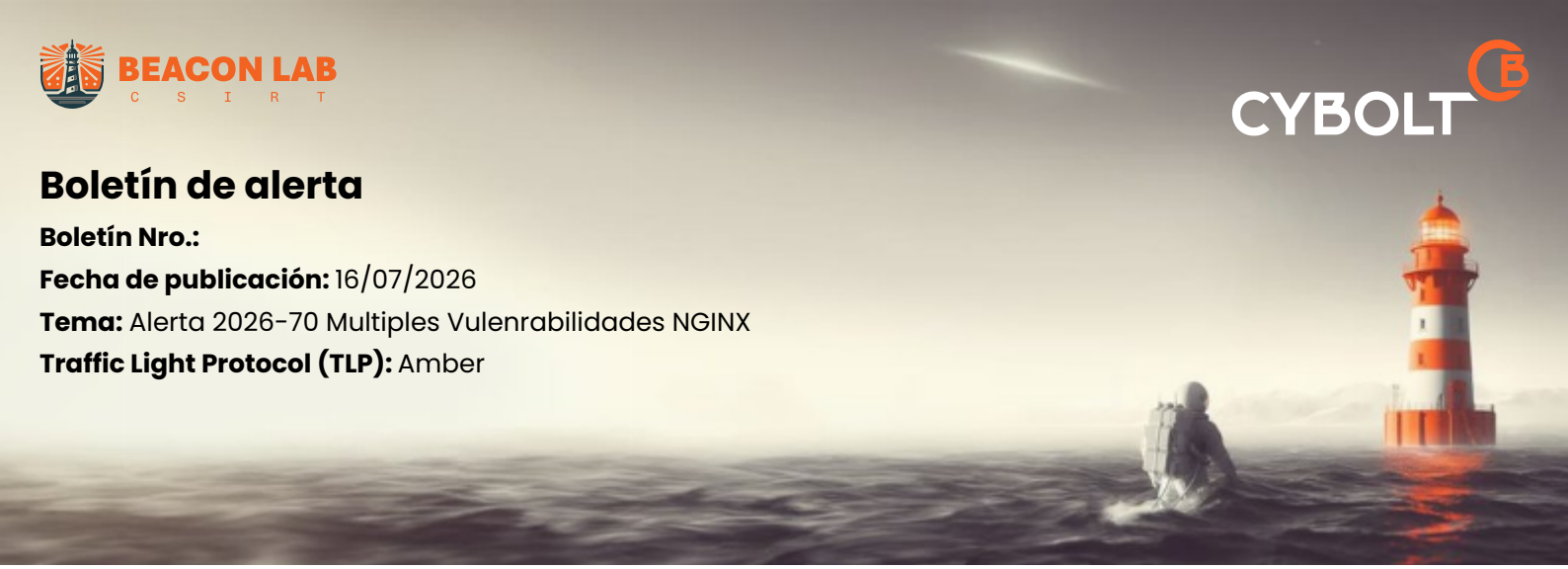

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 16/07/2026
Tema: Alerta 2026-70 Multiples Vulenrabilidades NGINX
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **NGINX Open Source**
  - 1.31.2 anteriores a 1.31.3
  - 1.30.x y versiones anteriores afectadas según el módulo correspondiente
- **NGINX Plus**
  - R37 anteriores a R37 P3
  - R36 anteriores a R36 P7
  - Algunas ramas anteriores (R33 y posteriores) según el módulo afectado.

Descripción

F5 publicó un conjunto de actualizaciones de seguridad para **NGINX Plus** y **NGINX Open Source** con el objetivo de corregir tres vulnerabilidades que afectan distintos módulos del servidor web. Aunque ninguna de ellas compromete directamente el plano de control (*control plane*), un atacante remoto podría provocar reinicios de procesos, divulgación limitada de memoria o modificaciones parciales de memoria bajo configuraciones específicas.

A continuación se describen las vulnerabilidades:

CVE-2026-42533 – Heap Buffer Overflow en el módulo map (CVSS 8.1): Esta vulnerabilidad consiste en un **Heap Buffer Overflow** dentro de la directiva **map** cuando se utilizan determinadas expresiones regulares y referencias a variables. Un atacante remoto podría enviar solicitudes especialmente diseñadas que desencadenen corrupción de memoria.

CVE-2026-56434 – Use-After-Free en ngx_http_ssi_module (CVSS 6.5): Esta vulnerabilidad afecta el módulo **ngx_http_ssi_module** cuando se utilizan simultáneamente las siguientes configuraciones: Server-Side Includes (SSI), proxy_pass y proxy_buffering off. En este escenario, un atacante con capacidad de realizar un ataque **Man-in-the-Middle (MITM)** sobre el servidor ascendente (*upstream*) podría provocar una condición **Use-After-Free**.

CVE-2026-60005 – Acceso a memoria no inicializada en ngx_http_slice_module (CVSS 7.5): Esta vulnerabilidad afecta el módulo **ngx_http_slice_module**, utilizado para servir archivos grandes mediante fragmentación (*slice*). Cuando la directiva **slice** está habilitada junto con determinadas expresiones regulares o durante actualizaciones de caché en segundo plano, un atacante remoto no autenticado puede provocar acceso a memoria no inicializada. El módulo **no está habilitado por defecto**, por lo que únicamente los servidores compilados con –with-http_slice_module son susceptibles.

Solución

F5 recomienda actualizar inmediatamente a las versiones corregidas de NGINX.

- **NGINX Open Source**
  - Actualizar a **1.31.3** o superior.
- **NGINX Plus**
  - Actualizar a **R37 P3** o superior.
  - Actualizar a **R36 P7** o superior si se mantiene esa rama de soporte.
- Medidas adicionales
  - Revisar si los módulos ngx_http_slice_module y ngx_http_ssi_module están habilitados.
  - Validar el uso de expresiones regulares complejas dentro de la directiva map.

Información adicional:

- F5 Security Advisory K000162098 (CVE-2026-56434)
- F5 Security Advisory K000162100 (CVE-2026-60005)
- NVD – CVE-2026-56434
- NVD – CVE-2026-60005
- NGINX Security Advisories