Boletín de alerta

Boletín Nro.: 32
Fecha de publicación: 31/03/2026
Tema: Alerta 2026-32 Vulnerabilidad críticas en productos NGINX
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- **NGINX Open Source**: Versiones 0.5.13 hasta 1.29.6.
- **NGINX Plus**: Afectado según módulos específicos habilitados.

Descripción

Se han identificado vulnerabilidades RCE críticas en productos NGINX que permiten denegación de servicio, ejecución de código arbitrario o escritura de archivos fuera del directorio raíz, identificadas como CVE-2026-27654 con CVSSv3.1 8.2, CVE-2026-32647 con CVSSv3.1 7.8 y CVE-2026-27651 con CVSSv3.1 7.5.

Las vulnerabilidades de mas importante y críticas se detallan a continuación**:**

CVE	Score	Descripción
CVE-2026-27654	8.2	Desbordamiento de búfer en ngx_http_dav_module vía métodos MOVE/COPY; permite DoS o modificación de archivos fuera de raíz.
CVE-2026-32647	7.8	Lectura/escritura fuera de límites en ngx_http_mp4_module con archivos MP4 maliciosos; permite DoS o ejecución de código local.
CVE-2026-27651	7.5	Desreferencia NULL en ngx_mail_auth_http_module (CRAM-MD5/APOP); provoca terminación de workers remotos.

Solución:

El fabricante recomienda actualizar los productos afectados a la versión estable más reciente desde nginx.org:

https://nginx.org/en/download.html

Mitigación:

- Deshabilita módulos innecesarios (dav, mp4, mail auth) hasta parchear.

- Monitorea logs por solicitudes sospechosas en endpoints afectados.

Información adicional:

- https://www.cve.org/CVERecord?id=CVE-2026-27654
- https://www.cve.org/CVERecord?id=CVE-2026-32647
- https://www.cve.org/CVERecord?id=CVE-2026-27651
- https://nginx.org/en/security_advisories.html