Boletín de alerta

Boletín Nro.: 22
Fecha de publicación: 11/03/2026
Tema: Alerta 2026-22 Vulnerabilidad Crítica en Nginx UI
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- **Nginx UI** en todas las versiones anteriores a **2.3.3.**

Descripción

Recientemente investigadores de seguridad y el propio proyecto de **Nginx UI** reportaron la vulnerabilidad **CVE-2026-27944**, una falla crítica con **CVSS 9.8**, que afecta al panel web de administración para servidores Nginx. Nginx UI es una interfaz gráfica que permite administrar configuraciones, certificados SSL y hosts virtuales del servidor Nginx mediante una consola web. La vulnerabilidad permite que **un atacante remoto sin autenticación descargue y descifre copias de seguridad completas del servidor**, lo que representa un riesgo severo para organizaciones que tengan esta interfaz expuesta a Internet.

El problema se origina en el endpoint **/api/backup**, el cual se encuentra accesible sin ningún mecanismo de autenticación. Un atacante puede enviar una solicitud HTTP a este endpoint y obtener una copia completa del backup del sistema administrado por Nginx UI. Dicho backup puede contener información altamente sensible como **credenciales de usuario, tokens de sesión, certificados TLS/SSL, claves privadas y configuraciones del servidor Nginx**.

Adicionalmente, la aplicación expone en el encabezado HTTP **X-Backup-Security** la **clave AES-256 y el vector de inicialización (IV)** utilizados para cifrar el backup, lo que elimina completamente la protección criptográfica del archivo descargado. De esta forma, un atacante puede **descargar y descifrar inmediatamente el backup sin autenticación ni interacción del usuario**, obteniendo secretos de infraestructura y credenciales que podrían permitir el compromiso completo del servidor o ataques posteriores como secuestro de sesiones, manipulación del tráfico o ataques man-in-the-middle mediante claves SSL robadas.

Solución y mitigaciones:

El fabricante ha solucionado la vulnerabilidad en **Nginx UI versión 2.3.3**, por lo que se recomienda **actualizar inmediatamente todas las instancias vulnerables** a esta versión o posterior. La actualización

corrige el endpoint vulnerable e introduce controles adecuados de autenticación para las operaciones relacionadas con backups. El parche se puede encontrar en el siguiente enlance:
https://github.com/0xJacky/nginx-ui/security/advisories/GHSA-g9w5-qffc-6762

En entornos donde la actualización inmediata no sea posible, se recomienda aplicar controles compensatorios para reducir el riesgo de explotación. Entre ellos se incluye:

- **restringir el acceso al panel de administración de Nginx UI únicamente desde redes internas o a través de VPN**,
- implementar **listas de control de acceso por IP**, y evitar exponer interfaces de administración directamente a Internet.
- revisar logs en busca de solicitudes sospechosas al endpoint **/api/backup** y **rotar credenciales administrativas, tokens de sesión y certificados TLS** en caso de sospecha de exposición de backups.

Información adicional:

- https://www.cert.gov.py/vulnerabilidad-en-productos-nginx/
- https://nvd.nist.gov/vuln/detail/CVE-2026-27944
- https://www.secpod.com/blog/critical-nginx-ui-flaw-exposes-server-backups-and-encryption-keys