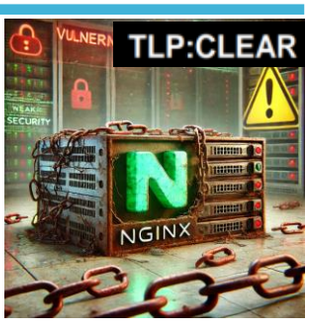
TIC

Advertencia de Seguridad

Actualización de Nginx para corregir vulnerabilidades

COLCERT AD-2309-020



Nginx es un servidor web de código abierto, que también puede actuar como proxy inverso, balanceador de carga y caché HTTP. Es conocido por su capacidad para manejar grandes volúmenes de tráfico con un bajo consumo de recursos, gracias a su arquitectura asincrónica y basada en eventos. Además, soporta protocolos modernos como HTTP/2 y conexiones seguras mediante SSL/TLS, lo que lo convierte en una herramienta fundamental para aplicaciones web de alto rendimiento.

Riesgos al utilizar versiones desactualizadas de Nginx:

Ausencia de actualizaciones de seguridad:
Exposición a vulnerabilidades conocidas que no serán corregidas

Ejecución Remota de Código (RCE):
Compromiso total del servidor, permitiendo acceso no autorizado, instalación de malware o control remoto de los recursos del servidor.

Vulnerabilidad a ataques de denegación de servicio (DoS):
Interrupción del servicio, afectando la disponibilidad del sitio web o aplicación.

Exposición de datos sensibles:
Violación de la confidencialidad de los datos, con potenciales consecuencias legales y pérdida de confianza de los usuarios.

Fugas de memoria y desbordamiento de búfer:
Posibilidad de ejecución de código no autorizado, corrupción de la memoria del servidor o fallos en el sistema.

Vulnerabilidad a inyecciones de código:
Modificación de la aplicación, acceso no autorizado a funciones del servidor y compromiso de la integridad de los datos.

Compatibilidad limitada con medidas de seguridad modernas:
El servidor puede utilizar configuraciones de seguridad débiles, como SSLv3, exponiendo las comunicaciones a ataques de intermediario (Man-in-the-Middle).

Explotación de vulnerabilidades de terceros:
Los atacantes pueden explotar vulnerabilidades de terceros (como OpenSSL o módulos adicionales) para comprometer el servidor.

Fuga de información en errores:
Exposición de información sensible sobre el servidor (mensajes de error más detallados que incluyen información sobre el servidor o la aplicación), versiones o configuración, que facilita el reconocimiento por parte de los atacantes.

Rendimiento degradado y falta de optimización:
Menor rendimiento y posibles interrupciones en el servicio, lo que afecta la experiencia del usuario.

Actualización Crítica de Seguridad en Nginx: Vulnerabilidad CVE-2024-7347 en ngx_http_mp4_module

Una nueva actualización de seguridad para Nginx ha sido lanzada para corregir una vulnerabilidad crítica de sobrelectura de búfer en el módulo ngx_http_mp4_module, identificada como CVE-2024-7347. Esta vulnerabilidad permite a atacantes remotos leer datos más allá de los límites del búfer, lo que podría exponer información sensible o comprometer la estabilidad del servidor. Las versiones anteriores de Nginx están afectadas, y se recomienda realizar una actualización inmediata a las versiones seguras más recientes.

COLCERT

Advertencia de Seguridad

Actualización de Nginx para Corregir Vulnerabilidades

COLCERT AD-2309-020

Impacto: Los servidores web que utilicen Nginx con el módulo MP4 pueden ser vulnerables a ataques que exploten esta falla, comprometiendo la confidencialidad y la disponibilidad de los servicios. La explotación de esta vulnerabilidad podría permitir a un atacante acceder a información sensible o causar la interrupción del servicio.

Medidas de mitigación:

Se recomienda actualizar a las versiones más recientes:

- ❑ Versión estable: Nginx 1.26.2
- ❑ Versión principal: Nginx 1.27.1

Pasos para actualizar Nginx:

1. **Verificar la versión actual:** Ejecuta el siguiente comando para verificar la versión de Nginx:

```
nginx -v
```

2. Actualizar en distribuciones basadas en Debian/Ubuntu.

```
•sudo apt update
•sudo apt install nginx
```

3. Actualizar en distribuciones basadas en Red Hat/CentOS:

```
sudo yum update sudo yum install nginx
```

4. **Actualizar Nginx desde código fuente:** Descarga la última versión de nginx.org. **Sigue el proceso habitual de compilación:**

```
tar -zxvf nginx-X.X.X.tar.gz
cd nginx-X.X.X
./configure
make
sudo make install
```

CVE relacionados con vulnerabilidades críticas en versiones desactualizadas de Nginx

CVE	Impacto	Versión corregida
CVE-2013-4547	Denegación de servicio (DoS)	1.5.6
CVE-2014-0133	Explotación remota de respuestas maliciosas	1.5.13
CVE-2016-0742	Ejecución remota de código (RCE)	1.9.10
CVE-2016-0746	Denegación de servicio (DoS)	1.9.11
CVE-2016-0747	Denegación de servicio (DoS)	1.9.11
CVE-2018-16843	Ejecución remota de código (RCE)	1.15.6
CVE-2018-16844	Denegación de servicio (DoS)	1.15.6
CVE-2018-16845	Denegación de servicio (DoS), Compromiso de seguridad	1.15.7
CVE-2021-23017	Ejecución remota de código (RCE)	1.21.0
CVE-2024-7347	Exposición de datos sensibles, Denegación de servicio (DoS)	1.26.2 y 1.27.1

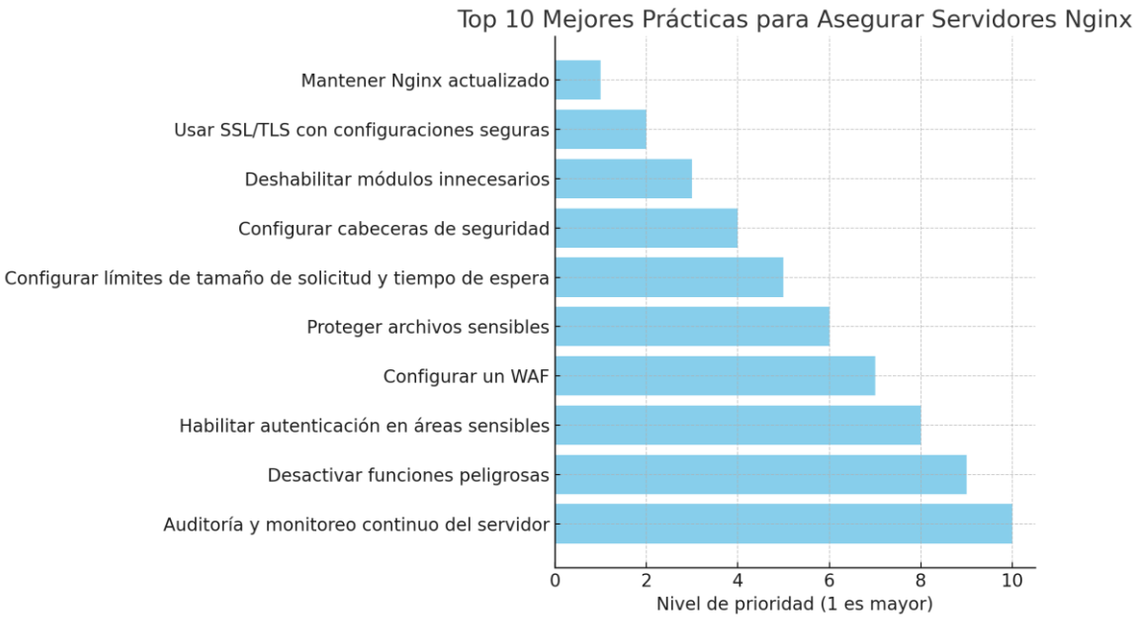
Fuente: https://cve.mitre.org

COLCERT

Advertencia de Seguridad

Actualización de Nginx para Corregir Vulnerabilidades

COLCERT AD-2309-020



La gráfica muestra las 10 mejores prácticas para asegurar servidores Nginx, organizadas en función de su prioridad, donde 1 representa la práctica más importante. Estas prácticas están diseñadas para reforzar la seguridad de los servidores Nginx y prevenir posibles amenazas y vulnerabilidades.

Recomendaciones

- Se recomienda actualizar a las versiones 1.26.2 (estable) o 1.27.1 (principal) para corregir la vulnerabilidad CVE-2024-7347.
- Implementar soluciones de monitoreo para identificar patrones anómalos y posibles intentos de explotación de vulnerabilidades en Nginx.
- Deshabilitar módulos innecesarios, aplicar encabezados de seguridad (como Strict-Transport-Security y Content-Security-Policy), y establecer límites de tamaño de solicitud para prevenir ataques de denegación de servicio (DoS).
- Limitar el acceso al servidor desde direcciones IP de confianza y proteger áreas sensibles con autenticación básica o autenticación multifactor.
- Verificar continuamente los registros de Nginx en busca de intentos de explotación o actividad sospechosa.
- Establecer un procedimiento de gestión de vulnerabilidades.

COLCERT

Advertencia de Seguridad

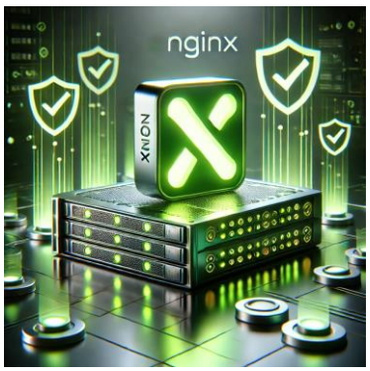
Actualización de Nginx para Corregir Vulnerabilidades

COLCERT AD-2309-020

NIVEL DE RIESGO

ALTO

"La actualización de NGINX es esencial para evitar la explotación de vulnerabilidades críticas, protegiendo el servidor de ataques que pueden comprometer tanto la disponibilidad como la confidencialidad de los datos sensibles."



FUENTES:

- CVE-2024-7347 – Vulnerabilidad de sobrelectura de búfer en el módulo MP4. - https://cve.mitre.org
- Documentación oficial de Nginx – https://nginx.org/en/docs/
- Nginx Vulnerability Information – National Vulnerability Database (NVD). - https://nvd.nist.gov
- Tenable Security Research – - https://www.tenable.com
- OWASP (Open Web Application Security Project) – https://owasp.org
- SANS Institute – Web Application Security and Nginx – https://www.sans.org
- Nginx Blog – Security Updates and Patching – https://www.nginx.com/blog/
- CIS Benchmarks – Nginx Hardening Guidelines – https://www.cisecurity.org/benchmark/nginx
- SecurityWeek – Vulnerabilities in Web Servers – https://www.securityweek.com
- Tenable Blog – Nginx Vulnerabilities and Exploits – https://www.tenable.com/blog
- DigitalOcean – Securing Nginx on Linux –
- Mitre ATT&CK Framework – https://attack.mitre.org
- Exploit Database – Nginx Vulnerabilities – https://www.exploit-db.com

COLCERT