Boletín de alerta

Boletín Nro.: 92
Fecha de publicación: 28/08/2026
Tema: Alerta 2026-92 Vulnerabilidad crítica RCE en Next.js para servidores Windows
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Paquete next/aplicaciones Next.js ejecutadas sobre un sistema de archivos Windows.
  - Versiones >= 13.4 y < 15.5.24.
  - Versiones >= 16.0 y < 16.3.3.

Descripción

Recientemente, se ha publicado una ulnerabilidad identificado como **CVE-2026-75604**, en Next.js, framework de React utilizado para desarrollar aplicaciones web renderizadas en servidor. La falla está clasificada como crítica, con una puntuación CVSS v3.1 de 9.0 y puede permitir ejecución remota de código (RCE) sin autenticación en servidores Windows.

La vulnerabilidad corresponde a CWE-22: Path Traversal. El manejo de rutas del caché incremental no limita correctamente ciertos valores manipulados al directorio de caché previsto. En Windows, el carácter de barra invertida (\) funciona como separador de directorios; una clave de caché especialmente creada puede aprovechar esa diferencia para resolver rutas fuera de la ubicación autorizada.

Como resultado, un atacante remoto podría provocar operaciones de lectura o escritura fuera del directorio de caché y llegar a influir en archivos que posteriormente sean ejecutados por el servidor. El impacto potencial incluye compromiso de confidencialidad, integridad y disponibilidad del servidor donde se aloja la aplicación.

La exposición se limita a despliegues sobre Windows con los routers indicados y sin Cache Components. Aun así, debido a que la explotación no requiere privilegios ni interacción de usuario, los entornos afectados deben considerarse de atención prioritaria.

Solución:

La medida recomendada es actualizar inmediatamente Next.js a una versión corregida: 15.5.24 para la rama 15.x o 16.3.3 para la rama 16.x, y volver a desplegar la aplicación.

Como medida temporal de defensa en profundidad, pueden habilitarse reglas de WAF que detecten intentos de explotación asociados a la CVE. Sin embargo, esto no sustituye la actualización. También se recomienda identificar aplicaciones Next.js ejecutándose en Windows, revisar la versión efectiva instalada en producción y verificar que las instancias actualizadas hayan sido desplegadas correctamente.

Puedes descargar el parche directamente del fabricante en el siguiente link: **advisory oficial de Next.js/Vercel.**

Información adicional:

- **https://github.com/vercel/next.js/security/advisories/GHSA-p293-qw3h-jr36**
- **https://security.snyk.io/vuln/SNYK-JS-NEXT-19269946**
- **https://developers.cloudflare.com/changelog/post/2026-08-26-emergency-waf-release/**