

Alert Bulletin

Bulletin N.: 92

Publication Date: 28/08/2026

Subject: Alert 2026-92 Critical RCE Vulnerability in Next.js for Windows Servers

Traffic Light Protocol (TLP): White

Affected product(s):

- Paquete next/aplicaciones Next.js ejecutadas sobre un sistema de archivos Windows.
 - Versiones ≥ 13.4 y $< 15.5.24$.
 - Versions ≥ 16.0 and $< 16.3.3$.

Description

Recently, a vulnerability identified as **CVE-2026-75604** has been published in Next.js, a React framework used to develop server-rendered web applications. The flaw is classified as critical, with a CVSS v3.1 score of 9.0 and can allow remote code execution (RCE) without authentication on Windows servers.

The vulnerability corresponds to CWE-22: Path Traversal. The path handling of the incremental cache does not properly restrict certain manipulated values to the intended cache directory. On Windows, the backslash character (`\`) works as a directory separator; a specially crafted cache key can exploit that difference to resolve paths outside the authorized location.

As a result, a remote attacker could cause read or write operations outside the cache directory and end up influencing files that are subsequently executed by the server. The potential impact includes compromise of confidentiality, integrity, and availability of the server hosting the application.

Exposure is limited to Windows deployments with the indicated routers and without Cache Components. Even so, because exploitation does not require privileges or user interaction, affected environments should be considered priority attention.

Solution:

The recommended measure is to immediately update Next.js to a fixed version: 15.5.24 for the 15.x branch or 16.3.3 for the 16.x branch, and redeploy the application.

As a temporary defense-in-depth measure, WAF rules can be enabled to detect exploitation attempts associated with the CVE. However, this does not replace the update. It is also recommended to identify

Next.js applications running on Windows, review the effective version installed in production, and verify that updated instances have been deployed correctly.

You can download the patch directly from the manufacturer at the following link: [official Next.js/Vercel advisory](#).

Additional information:

- <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/>