GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

2 September 2026

Advisory 227: Next.js Path Traversal on Windows-Hosted Servers Leading to Remote Code Execution (CVE-2026-75604).

Release Date: 1st September 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators and developers that build or host web applications using the Next.js framework, particularly where the application is deployed on Windows-based servers. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-75604 (CVSS 3.1 base score 9.0, Critical) is a path traversal vulnerability (CWE-22) in Next.js, the widely used React web application framework. On Windows-hosted servers, Next.js applications using the Pages Router or App Router without Cache Components do not consistently escape backslashes in route segments before constructing incremental-cache file paths. A remote, unauthenticated attacker can supply encoded Windows path separators in a request to traverse outside the intended cache root directory.

Successful traversal exposes private build data, including the server-reference-manifest encryption key. Disclosure of that key can, in turn, be leveraged to achieve remote code execution against the affected application. Exploitation requires no authentication or user interaction, though attack complexity is rated High because it depends on the application being hosted on a Windows server with the vulnerable code path in use.

What are the systems affected?

The following version(s) are affected:

- Next.js 13.4.0 up to (but not including) 15.5.24, and 16.3.3-prerelease builds prior to the fix – (Affected, when hosted on Windows-based servers)

Next.js 15.5.24 and 16.3.3 and later - (Not affected, patched)

This vulnerability is specific to Windows-hosted deployments; Next.js applications hosted on Linux or macOS servers are not affected by this particular flaw. Organizations should first confirm the hosting platform of each Next.js application before treating it as affected, and should not assume that only a Linux/macOS hosting posture is a substitute for patching if the hosting platform is Windows or unknown.

What does this mean?

Typical attack flow:

1. **Identify a Windows-hosted Next.js application**
    - An attacker identifies a Next.js application, using the Pages Router or App Router without Cache Components, running on a Windows-hosted server.
2. **Traverse the incremental cache and extract the encryption key**
    - The attacker sends a crafted request containing encoded Windows path separators in a route segment, exploiting inconsistent backslash escaping to traverse outside the intended cache root and read private build data, including the server-reference-manifest encryption key, then uses that key to achieve remote code execution against the application.

Attack vectors:

- Direct network requests to a vulnerable, Windows-hosted Next.js application — no authentication or user interaction is required.
- Any internet-facing Next.js deployment on Windows using an affected version and the vulnerable routing/caching code path.

Successful exploitation may allow attackers to:

- Read private build data outside the intended cache directory, including the server-reference-manifest encryption key.
- Leverage the disclosed encryption key to achieve remote code execution against the affected application.

Mitigation process

CERTVU recommends the following:

1. Upgrade Next.js without delay

    - Update every affected, Windows-hosted Next.js application to 15.5.24 or 16.3.3 (or later), given the maximum-severity impact and the lack of any authentication precondition.

2. Confirm the hosting platform of every Next.js application
3. Rotate the server-reference-manifest encryption key after patching
4. Audit the estate for the affected product
5. Conduct a compromise assessment

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://github.com/vercel/next.js/security/advisories/GHSA-p293-qw3h-jr36
2. https://www.cve.org/CVERecord?id=CVE-2026-75604