Blog / Changelog

Next.js May 2026 security release

Jimmy Lai Head of Next.js

2 min read

May 7, 2026

Summary

We have shipped a coordinated security release for Next.js addressing 13 advisories across denial of service, middleware and proxy bypass, server-side request forgery, cache poisoning, and cross-site scripting. One advisory addresses an upstream React Server Components vulnerability tracked as CVE-2026-23870.

Recommended actions

Patched versions are available for both React and Next.js, and all affected users should upgrade immediately.

Impact

The release addresses the following advisories:

Middleware and proxy bypass

Affects applications that rely on `middleware.js` or `proxy.js` for authorization.

- **High**: Auth bypass via App Router segment-prefetch URL
- **High**: App Router segment-prefetch bypass, incomplete fix follow-up

- **High**: Pages Router i18n default-locale path bypasses proxy authorization
- **High**: Bypass via dynamic route parameter injection
- **Low**: Middleware redirects can be cache-poisoned

Denial of service

Affects applications using Server Functions, Partial Prerendering with Cache Components, or the Image Optimization API.

- **High**: DoS in React Server Components (tracked upstream as CVE-2026-23870)
- **High**: DoS via connection exhaustion in applications using Cache Components
- **Moderate**: DoS via the Image Optimization API

Server-side request forgery

Affects applications that handle WebSocket upgrade requests.

- **High**: SSRF in applications using WebSocket upgrades

Cache poisoning

Affects applications with caching layers in front of React Server Component responses.

- **Moderate**: Cache poisoning in React Server Component responses
- **Low**: Cache poisoning via collisions in RSC cache-busting

Cross-site scripting

Affects applications using CSP nonces in App Router, or `beforeInteractive` scripts that consume untrusted input.

- **Moderate**: XSS in App Router applications using CSP nonces
- **Moderate**: XSS in beforeInteractive scripts with untrusted input

Resolution

These vulnerabilities are addressed by the patched releases of React and Next.js. Patching is the only complete mitigation, and all affected users should upgrade immediately.

Vercel has not deployed new WAF rules for this release; these advisories cannot be reliably blocked at the WAF layer.

Affected versions

Fixed in

- Next.js: 15.5.18 16.2.6

- **React**: `19.0.6`, `19.1.7`, `19.2.6` for the `react-server-dom-parcel`, `react-server-dom-webpack` and `react-server-dom-turbopack` packages

Frameworks and bundlers using `react-server-dom-*` packages should install the latest versions provided by their respective maintainers.

References

- Upstream React advisory (CVE-2026-23870)