Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Unauthenticated RCE in React Server Components

Date of Publication	Admiralty Code	TA Number
November 10, 2026	A1	TA2026332

Summary

First Seen: October 14, 2026
Affected Products: React Server Components (react-server-dom-webpack, react-server-dom-parcel, react-server-dom-turbopack), Vercel Next.js
Impact: Successful exploitation allows a remote, unauthenticated attacker to run server-side functions within an affected application. The resulting damage depends on the Server Actions exposed, which commonly handle orders, account changes, record updates, file operations, and calls to internal services. This can lead to data theft, tampering with business records, and a foothold into connected back-end systems. As React Server Components and Next.js commonly power customer-facing websites, storefronts, and SaaS platforms, and a public exploit lowers the skill required to attack them, the business risk is high for organizations running unpatched applications despite the narrow trigger conditions.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
Unassigned	React Server Components Typed Array Deserialization Remote Code Execution Vulnerability (GHSA-xqc2-xf4c-x3h3)	React Server Components (react-server-dom-webpack, react-server-dom-parcel, react-server-dom-turbopack)	✗	✗	✓

Vulnerability Details

#1 A critical unauthenticated remote code execution vulnerability in the React Server Components (RSC) serializer, the component that encodes and decodes server-rendered and cached data. React has not assigned a CWE; it is assessed here as CWE-502 (Deserialization of Untrusted Data).

#2 The flaw stems from improper handling of typed arrays during deserialization. When a cached response contains multiple typed-array views over a single shared ArrayBuffer, the RSC decoder becomes desynchronized from the serialized stream. An attacker-controlled value in the same response is then treated as trusted content, allowing the decoder to be steered into invoking a Server Action with attacker-supplied arguments.

#3 Exploitation requires a response that carries multiple typed arrays alongside an attacker-controlled value, a condition React describes as extremely rare. In Next.js, this corresponds to a "use cache" function returning multiple typed arrays and user-influenced data on a cached page that can resolve a Server Action. The attack is delivered over the network through a crafted request, and its impact depends on the Server Action invoked. As the defect resides in React's serializer, securely written application code can still be exposed.

#4 React rates the issue Critical with a CVSS v4.0 score of 9.5, reflecting network exploitability, low attack complexity, no required privileges or user interaction, and high impact on the vulnerable and connected systems.

#5 Affected versions of react-server-dom-webpack, react-server-dom-parcel, and react-server-dom-turbopack are 19.0.0 to 19.0.8, 19.1.0 to 19.1.9, 19.2.0 to 19.2.8, and 19.3.0, fixed in 19.0.9, 19.1.10, 19.2.9, and 19.3.1. Next.js 16.0.0 to 16.4.0 using the App Router with Cache Components is also affected and is fixed in 16.4.1. Applications that do not use a server, or a framework, bundler, or bundler plugin supporting React Server Components, are not affected.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
Unassigned	React react-server-dom-webpack (19.0.0 to 19.0.8, 19.1.0 to 19.1.9, 19.2.0 to 19.2.8, 19.3.0)	cpe:2.3:a:facebook:react-server-dom-webpack:*:*:*:*:*:node.js:*:*	CWE-502
	React react-server-dom-parcel (19.0.0 to 19.0.8, 19.1.0 to 19.1.9, 19.2.0 to 19.2.8, 19.3.0)	cpe:2.3:a:facebook:react-server-dom-parcel:*:*:*:*:*:node.js:*:*	
	React react-server-dom-turbopack (19.0.0 to 19.0.8, 19.1.0 to 19.1.9, 19.2.0 to 19.2.8, 19.3.0)	cpe:2.3:a:facebook:react-server-dom-turbopack:*:*:*:*:*:node.js:*:*	
	Vercel Next.js (16.0.0 to 16.4.0, App Router with Cache Components)	cpe:2.3:a:vercel:next.js:*:*:*:*:*:node.js:*:*	

Recommendations

Upgrade React Server Components Packages: Update react-server-dom-webpack, react-server-dom-parcel, and react-server-dom-turbopack to 19.0.9, 19.1.10, 19.2.9, 19.3.1, or later. React provides no workaround and recommends upgrading immediately, so prioritize internet-facing applications built on Server Components.

Upgrade Next.js Deployments: Update Next.js 16.0.0 through 16.4.0 to 16.4.1 or later, prioritizing applications that use the App Router with Cache Components. Rebuild and redeploy so the patched RSC runtime is included in production artifacts.

Verify the Fix in Deployed Builds: Search the react-server-dom-webpack server production bundle for the getBackingBlob marker across container images, serverless bundles, and cached build outputs. Zero matches indicates a build that is still vulnerable.

Apply Interim Mitigations: Where patching is delayed, remove or refactor "use cache" functions that return multiple typed arrays together with attacker-controlled values. Enforce server-side authentication, authorization, and input validation within every Server Action to limit the impact of any unauthorized invocation.

Monitor for Exploitation Attempts: Review web server, CDN, and application logs for requests with unusually long base64-encoded query parameters and for responses containing serialized Server Action output. Configure WAF or reverse-proxy rules to flag such requests to RSC-rendered routes, and escalate suspicious activity to incident response.

Strengthen Vulnerability Management: Maintain a software bill of materials covering direct and transitive dependencies on React Server Components and frameworks such as Next.js. Track vendor security advisories and prioritize critical fixes even when no CVE has been assigned.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1594: Search Victim-Owned Websites	
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript

Patch Links

https://github.com/react/react/security/advisories/GHSA-xqc2-xf4c-x3h3

https://github.com/vercel/next.js/security/advisories/GHSA-673q-mjm6-r5xr

https://nextjs.org/blog/nextjs-security-update-october-14-2026

https://github.com/vercel/next.js/commit/a4cea6aec5da89d116b8960e113189cf51745d2f

References

https://github.com/react/react/security/advisories/GHSA-xqc2-xf4c-x3h3

https://github.com/briskets/GHSA-xqc2-xf4c-x3h3-rce-poc

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 10, 2026 • 07:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com