CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

Friday, December 5, 2025

CAL-CSIC-202512-A -003

Critical RCE Exposure in React Server Components and Next.js

Multiple Sectors impacted	React Server Components	RCE	PoC Available

The California Cybersecurity Integration Center has identified two critical remote code execution (RCE) vulnerabilities affecting the React Server Components (RSC) "Flight" protocol and the Next.js App Router.[1] CVE-2025-55182 and CVE-2025-66478 are both rated CVSS 3.1 score 10.0 and stem from insecure deserialization flaws that allow unauthenticated attackers to submit maliciously crafted HTTP requests to vulnerable server-side RSC endpoints. Successful exploitation enables arbitrary code execution on the underlying server, with full compromise of confidentiality, integrity, and availability.

CVE-2025-55182 affects React Server Components in versions **19.0.0, 19.1.0, 19.1.1, and 19.2.0** across packages such as react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. Because many frameworks embed these components, dependent ecosystems, including Next.js App Router, Vite's RSC plugin, Parcel RSC plugin, React Router RSC preview, and Waku, are also exposed. A public PoC exists and exploitation has been demonstrated with high reliability in controlled settings. While no widespread exploitation has been confirmed, active scanning is underway, and mass exploitation is assessed as likely. CISA has added this CVE to their Known Exploited Vulnerability (KEV) catalog.[2]

CVE-2025-66478 affects Next.js App Router deployments in versions **≥14.3.0-canary.77**, **≥15**, and **≥16**, all of which bundle vulnerable RSC code. The App Router is enabled by default, significantly expanding the attack surface. Researchers have developed functioning PoCs with near-100% success rates in default configurations. No confirmed widespread exploitation has been reported as of December 2025, but the vulnerability requires no authentication, is trivially reachable in typical deployments, and is expected to see rapid adoption in automated exploitation campaigns.

Both vulnerabilities carry global exposure risk due to widespread adoption of React and Next.js. Wiz reports that 39% of cloud environments contain vulnerable React or Next.js versions. Given the popularity of these frameworks, React being used by over 80% of surveyed developers, the number of internet-facing vulnerable servers is assessed as very high, with potentially millions of affected applications worldwide.

Patches are available and immediate upgrades are strongly recommended.

- React: 19.0.1, 19.1.2, 19.2.1
- Next.js**:** 15.0.5, 15.1.9, 15.2.6, 15.3.6, 15.4.8, 15.5.7, 16.0.7

Organizations using React Server Components, Next.js App Router, or RSC-dependent frameworks should assume exposure and prioritize immediate patching, external surface scanning, and log review for suspicious RSC-related requests.

The Cal-CSIC recommends immediately applying the patches released by React developers in the following versions: 19.0.1, 19.1.2, and 19.2.1.

For further information on on this, please see the react developers blogpost[3]

References

[1] Pics Security; "React2Shell RCE Vulnerability; CVE-2025-55182 and CVE-2025-66478 explained"; https://www.picussecurity.com/resource/blog/react-flight-protocol-rce-vulnerability-cve-2025-55182-and-cve-2025-66478-explained; accessed 05 December 2025

[2] CISA; "CISA Adds One Known Exploited Vulnerability to Catalog"; https://www.cisa.gov/news-events/alerts/2025/12/05/cisa-adds-one-known-exploited-vulnerability-catalog; accessed 05 December 2025

[3] React; "Critical Security Vulnerability in React Server Components"; https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components; accessed 50 December 2025

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.