

What is React2Shell?

React2Shell is the name for CVE-2025-55182, an unauthenticated remote code execution flaw in React Server Components disclosed on December 3, 2025 with a CVSS score of 10.0. React decodes the payloads sent to Server Function endpoints, and a crafted request could make that deserialization run attacker code on the server. It affected react-server-dom-webpack, -parcel and -turbopack 19.0 to 19.2.0 and frameworks built on them, most visibly Next.js. Fixed in React 19.0.1, 19.1.2 and 19.2.1; CISA added it to the KEV catalog on December 5, 2025.

HOW IT WORKS

01 How the attack worked

Shown for defensive context, the attack needed only network access to the app:

- One POST request to a Next.js route that accepts Server Function calls, recognizable by the Next-Action header and a multipart or text body in React's serialization format.
- A crafted payload whose structure abuses how references are resolved during deserialization, steering the server into executing attacker-chosen JavaScript in the Node.js process.
- No login, no user interaction. The vulnerable code runs before any application logic checks who is calling.

Public exploits appeared within days of the advisory and mass scanning followed. CISA added the CVE to its Known Exploited Vulnerabilities catalog on December 5, 2025, two days after disclosure. Follow-up fixes in December 2025 and January 2026 addressed related denial-of-service bugs (CVE-2025-55184, CVE-2025-67779, CVE-2026-23864) and a source-code exposure bug (CVE-2025-55183), so "patched for React2Shell" is not the same as current.

HOW TO DEFEND

- React RSC packages: at least 19.0.1, 19.1.2 or 19.2.1 for CVE-2025-55182, and preferably the latest patch release in your line, which also covers the follow-up denial-of-service and source-exposure bugs.
- Next.js: the latest patch release in your minor line. The official Next.js and React advisories list the exact versions per line.
- Rotate secrets on any app that ran a vulnerable version while exposed to the internet, since code execution in the Node.js process exposes environment variables and cloud credentials.
- Hunt for unexpected child processes from the Node.js server, outbound connections to unknown hosts and new files in writable directories.

SOURCES

- [1] React: Critical security vulnerability in React Server Components
- [2] Next.js: CVE-2025-66478 advisory
- [3] NVD: CVE-2025-55182
- [4] MITRE CWE-502: Deserialization of Untrusted Data

Find the path to a shell before an attacker does.

securelayer7.net/learn/web-exploitation/what-is-react2shell

[Open online](https://securelayer7.net/learn/web-exploitation/what-is-react2shell)