Security Advisory 2025-041

Critical Security Vulnerability in React Server Components

2025-12-04 — v1.0

TLP:CLEAR

History:

- *04/12/2025 — v1.0 – Initial publication*

Summary

On December 3, 2025, the React Team publicly disclosed a critical security vulnerability affecting React Server Components (RSC) and related packages. The vulnerability allows for unauthenticated remote code execution (RCE) via maliciously crafted HTTP requests [1].

It is recommended to update all affected component packages and any frameworks that integrate them.

Technical Details

The vulnerability **CVE-2025-55182**, with a CVSS score of 10, is due to unsafe deserialisation of payloads from HTTP requests to React Server Function endpoints. It allows for unauthenticated remote code execution (RCE) via maliciously crafted HTTP requests [1].

React Server Functions allow a client to call a function on a server. React provides integration points and tools that frameworks and bundlers use to help React code run on both the client and the server. React translates requests on the client into HTTP requests which are forwarded to a server. On the server, React translates the HTTP request into a function call and returns the needed data to the client [1].

Affected Products

The vulnerability is present in versions 19.0, 19.1.0, 19.1.1, and 19.2.0 of the following React Server Components packages:

- react-server-dom-webpack
- react-server-dom-parcel
- react-server-dom-turbopack

Any framework or tool that integrates React Server Components using the affected packages may inherit the vulnerability.

Confirmed affected ecosystem components include:

- **Next.js App Router** (multiple impacted versions)
- **RSC plugin for Vite**
- **RSC plugin for Parcel**
- **React Router's unstable RSC APIs**
- **Redwood SDK**
- **Waku**
- Any third-party project bundling vulnerable `react-server-dom-*` packages

Recommendations

It is recommended updating affected React Server Components packages to a fixed version (19.0.1, 19.1.2, or 19.2.1) as soon as possible.

Depending on the affected ecosystem in use, the React Team provided additional instruction [1].

References

[1] https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components