GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

11 December 2025

Advisory 114: Critical remote code execution (RCE) vulnerability

Release Date: 03rd of December 2025
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

- CVE-2025-55182 (also dubbed "React2Shell") is a critical remote-code-execution (RCE) vulnerability in React Server Components (RSC).
- The vulnerability stems from unsafe deserialization of incoming HTTP request payloads in the "Flight" protocol handling RSC — malformed or malicious payloads can trigger arbitrary code execution on the server.

What are the Systems affected?

• React Server Components — specifically packages react-server-dom-webpack, react-server-dom-parcel, and react-server-dom-turbopack, in versions 19.0.0, 19.1.0, 19.1.1, 19.2.0.

• Frameworks and tools built on top of React RSC, including Next.js (versions 15.x and 16.x with App Router), and other RSC-enabled bundlers/plugins (e.g. Vite RSC plugin, Parcel RSC plugin, RedwoodSDK, Waku, React Router RSC mode).

What does this mean?

How attackers exploit this vulnerability (attack vector)

- An unauthenticated attacker sends a specially crafted HTTP request to an RSC "Server Function" endpoint.
- Because the server improperly handles/deserializes the request data, the attacker-controlled payload triggers server-side execution of arbitrary JavaScript code — meaning full remote code execution under the server's privileges.

Mitigation process

CERTVU recommend:

Patch Immediately

Update React Server Components packages to fixed versions: react-server-dom- → version **19.0.1**, **19.1.2**, or **19.2.1**.

Reference

.

1. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-vulnerability-in-react-server-components-cve-2025-55182
2. https://www.cve.org/CVERecord?id=CVE-2025-55182