React Server Components and Next.js Vulnerable to Critical (10.0) Remote Code Execution Vulnerability (CVE-2025-55182)

This report is distributed as **TLP:AMBER+STRICT**. Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.

Disclaimer | CyberAlberta

Summary

On 3 December 2025, React disclosed the critical remote code execution (RCE) vulnerability CVE-2025-55182 affecting multiple React Server Components (RCS) packages and the broader ecosystem of frameworks that rely on the React Flight protocol. Consequently, Next.js disclosed a downstream critical vulnerability labelled as CVE-2025-66478, which has since been rejected as a duplicate of CVE-2025-55182 as it is affected by the same flaw.

Details

CVE-2025-55182 – Critical (10.0): A remote code execution (RCE) vulnerability affecting RCS packages. A remote unauthenticated attacker can exploit this vulnerability by sending specially crafted HTTP requests to any Server Function endpoint, which triggers insecure deserialization in React and results in RCE on the server.

There is currently no evidence of active exploitation. However, researchers at Wiz stated their internally developed proof-of-concept (PoC) exploit achieved near-100% reliability in testing.[1] CyberAlberta Threat Intelligence is aware of scanning tools to identify vulnerable packages in code repositories and a claimed PoC exploit code that has since been revealed as AI-generated and non-functional.

Affected Products

CVE-2025-55182 affects the following products:

- Versions 19.0, 19.1.0. 19.1.1 and 19.2.0 of:
  - react-server-dom-webpack
  - react-server-dom-parcel
  - react-server-dom-turbopack
- Versions 15.x, 16.x, 14.3.0-canary.77 (and later canary releases) of:
  - Next.js
- Other frameworks that bundle the vulnerable packages include:
  - React Router (RSC mode)
  - Expo
  - Vite RSC plugin
  - Parcel RSC plugin

[1] https://www.wiz.io/blog/critical-vulnerability-in-react-cve-2025-55182#:~:text=Exploitation%20requires%20only%20a%20crafted%20HTTP%20request

- RedwoodSDK
- Waku

CyberAlberta Threat Intelligence identified 7 assets under the GoA's ASN hosting React products

IP	Domain
142.229.173.250	api.iam.alberta.ca
142.229.236.67	No response
142.229.45.250	api.iam.alberta.ca
142.229.236.69	auth.iam.alberta.ca
142.229.246.241	auth.iam.alberta.ca
199.213.74.50	applyalberta.ca
142.229.227.153	albertafirebans.ca

Figure 1 - Potentially Vulnerable Assets

It is currently unclear what the level of exposure these assets currently face. `applyalberta.ca` and `albertafirebans.ca` both appear to be publicly accessible. The remainder appear to be behind a login portal.

Assessment

CyberAlberta Threat Intelligence assess that wide-spread active exploitation of CVE-2025-55182 is likely imminent. Details about the vulnerability are steadily emerging and the development of PoC exploit code is already underway.

Recommendations

To defend exploitation of the reported vulnerabilities, it is recommended to:

- Assess the level of exposure of the identified GoA assets
- Assess codebase for use of any use of the vulnerable `react-server-dom*` packages.
- Patch React systems to the latest versions:
  - 19.0.1[2]
  - 19.1.2[3]
  - 19.2.1[4]
- Patch Next,js systems to the latest versions:
  - 15.0.5
  - 15.1.9
  - 15.2.6
  - 15.3.6
  - 15.4.8
  - 15.5.7

[2] https://github.com/facebook/react/releases/tag/v19.0.1
[3] https://github.com/facebook/react/releases/tag/v19.1.2
[4] https://github.com/facebook/react/releases/tag/v19.2.1

- 16.0.7

Next.js have provided guidance on applying updates in their security advisory.[5]

If Next.js cannot currently be upgraded, it is recommended to downgrade to the latest stable 14.x release using the command

```
npm install next@14
```

- Apply any available updates for other implicated frameworks:
  - Vite RSC plugin
  - Parcel RSC plugin
  - React Router RSC preview
  - Expo
  - RedwoodSDK
  - Waku

Next.js also provided guidance on updating these implicated frameworks in their security advisory.[6]

Further Detail

React disclosure: https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

Next,js blog: https://nextjs.org/blog/CVE-2025-66478

Wiz Blog: https://www.wiz.io/blog/critical-vulnerability-in-react-cve-2025-55182

Aikido Blog: https://www.aikido.dev/blog/react-nextjs-cve-2025-55182-rce

AWS Alert: https://aws.amazon.com/security/security-bulletins/rss/aws-2025-030/

Google Cloud Security & Identity Blog: https://cloud.google.com/blog/products/identity-security/responding-to-cve-2025-55182

[5] https://nextjs.org/blog/CVE-2025-66478#required-action

[6] https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components#update-react-router