

Admins and defenders gird themselves against maximum-severity server vuln



“I usually don’t say this, but patch right freakin’ now,” one researcher wrote. “The React CVE listing (CVE-2025-55182) is a perfect 10.”

React versions 19.0.1, 19.1.2, or 19.2.1 contain the vulnerable code. Third-party components known to be affected include:

- Vite RSC plugin
- Parcel RSC plugin
- React Router RSC preview
- RedwoodSDK
- Waku
- Next.js

According to Wiz and fellow security firm Aikido, the vulnerability, tracked as CVE-2025-55182, resides in Flight, a

protocol found in the React Server Components. Next.js has assigned the designation CVE-2025-66478 to track the vulnerability in its package.

The vulnerability stems from unsafe deserialization, the coding process of converting strings, byte streams, and other “serialized” formats into objects or data structures in code. Hackers can exploit the insecure deserialization using payloads that execute malicious code on the server. Patched React versions include stricter validation and hardened deserialization behavior.

“When a server receives a specially crafted, malformed payload, it fails to validate the structure correctly,” Wiz explained. “This allows attacker-controlled data to influence server-side execution logic, resulting in the execution of privileged JavaScript code.”

The company added:

In our experimentation, exploitation of this vulnerability had high fidelity, with a near 100% success rate and can be leveraged to a full remote code execution. The attack vector is unauthenticated and remote, requiring only a specially crafted HTTP request to the target server. It affects the default configuration of popular frameworks.

Both companies are advising admins and developers to upgrade React and any dependencies that rely on it. Users of any of the Remote-enabled frameworks and plugins mentioned above should check with the maintainers for guidance. Aikido also suggests admins and developers scan their codebases and repositories for any use of React using this link.

<https://arstechnica.com/security/2025/12/admins-and-defenders-gird-themselves-against-maximum-severity-server-vulnerability/>