

# Denial of Service Vulnerability in React Server Components

**High** zpao published GHSA-479c-33wc-g2pg 1 hour ago

## Package

**react-server-dom-parcel** ([npm](#)).

### Affected versions

19.0.0, 19.0.1, 19.0.2, 19.0.3, 19.0.4, 19.1.0,  
19.1.1, 19.1.2, 19.1.3, 19.1.4, 19.1.5 19.2.0,  
19.2.1, 19.2.2, 19.2.3, 19.2.4

### Patched versions

19.0.5, 19.1.6, 19.2.5

**react-server-dom-turbopack** ([npm](#)).

19.0.0, 19.0.1, 19.0.2, 19.0.3, 19.0.4, 19.1.0,  
19.1.1, 19.1.2, 19.1.3, 19.1.4, 19.1.5 19.2.0,  
19.2.1, 19.2.2, 19.2.3, 19.2.4

19.0.5, 19.1.6, 19.2.5

**react-server-dom-webpack** ([npm](#)).

19.0.0, 19.0.1, 19.0.2, 19.0.3, 19.0.4, 19.1.0,  
19.1.1, 19.1.2, 19.1.3, 19.1.4, 19.1.5 19.2.0,  
19.2.1, 19.2.2, 19.2.3, 19.2.4

19.0.5, 19.1.6, 19.2.5

## Description

### Impact

A denial of service vulnerability exists in React Server Components, affecting the following packages: react-server-dom-parcel, react-server-dom-turbopack, react-server-dom-webpack versions 19.0.0, 19.1.0 and 19.2.0. The vulnerability is triggered by sending specially crafted HTTP requests to Server Function endpoints.

The payload of the HTTP request causes excessive CPU usage for up to a minute ending in a thrown error that is catchable.

We recommend updating immediately.

The vulnerability exists in versions 19.0.0 through 19.0.4, 19.1.0 through 19.1.5, and 19.2.0 through 19.2.4 of:

[react-server-dom-webpack](#)

[react-server-dom-parcel](#)

[react-server-dom-turbopack](#)

## Patches

---

Fixes were back ported to versions 19.0.5, 19.1.6, and 19.2.5.

If you are using any of the above packages please upgrade to any of the fixed versions immediately.

If your app's React code does not use a server, your app is not affected by this vulnerability. If your app does not use a framework, bundler, or bundler plugin that supports React Server Components, your app is not affected by this vulnerability.

## References

---

See the [blog post](#) for more information and upgrade instructions.

### Severity

**High** 7.5 / 10

#### CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

[Learn more about base metrics](#)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

### CVE ID

CVE-2026-23869

### **Weaknesses**

- ▶ CWE-400
- ▶ CWE-502