# Denial of Service Vulnerabilities in React Server Components

High zpao published GHSA-83fc-fqcc-2hmg on Jan 26

Package

**react-server-dom-parcel** (npm)

| Affected versions | Patched versions |
| --- | --- |
| 19.0.0, 19.0.1, 19.0.2, 19.0.3, 19.1.0, 19.1.1, 19.1.2, 19.1.3, 19.1.4, 19.2.0, 19.2.1, 19.2.2, 19.2.3 | 19.0.4, 19.1.5, 19.2.4 |

**react-server-dom-turbopack** (npm)

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

**react-server-dom-webpack** (npm)

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

Description

## Impact

It was found that the fixes to address DoS in React Server Components were incomplete and we found multiple denial of service vulnerabilities still exist in React Server Components.

We recommend updating immediately.

The vulnerability exists in versions 19.0.0, 19.0.1, 19.0.2, 19.0.3, 19.1.0, 19.1.1, 19.1.2, 19.1.3, 19.1.4, 19.2.0, 19.2.1, 19.2.2, 19.2.3 of:

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

The vulnerabilities are triggered by sending specially crafted HTTP requests to Server Function endpoints, and could lead to server crashes, out-of-memory exceptions or excessive CPU usage; depending on the vulnerable code path being exercised, the application configuration and application code.

## Patches

Fixes were back ported to versions 19.0.4, 19.1.5, and 19.2.4.

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-2026-23864

### Weaknesses

- CWE-400
- CWE-502

### Credits

- mufeedvh — Reporter
- Ry0taK — Reporter
- jviide — Reporter
- marckwei — Reporter