

CVE-2025-55182

Meta React Server Components Remote Code Execution Vulnerability

Exigent CISA KEV since Dec 5, 2025 Actively exploited Ransomware use known Public exploit module (Metasploit)

A pre-authentication remote code execution vulnerability exists in React Server Components versions 19.0.0, 19.1.0, 19.1.1, and 19.2.0 including the following packages: react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. The vulnerable code unsafely deserializes payloads from HTTP requests to Server Function endpoints.

EVRS 97/100 Immediate priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.998 99.96th percentile · FIRST	CISA DEADLINE Dec 12, 2025 CISA federal deadline · Overdue by 10 months
--	---	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.998 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** Check for signs of potential compromise on all internet accessible REACT instances after applying mitigations.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
react	19.0.0 19.1.0 19.1.1 19.2.0	no fixed version listed	NVD
next.js	≥ 15.0.0 < 15.0.5 ≥ 15.1.0 < 15.1.9 ≥ 15.2.0 < 15.2.6 ≥ 15.3.0 < 15.3.6 ≥ 15.4.0 < 15.4.8 ≥ 15.5.0 < 15.5.7 ≥ 16.0.0 < 16.0.7 14.3.0 15.6.0 16.0.0	15.0.5 · 15.1.9 · 15.2.6 · 15.3.6 · 15.4.8 · 15.5.7	NVD

Sources

Vendor guidance react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

NVD nvd.nist.gov/vuln/detail/CVE-2025-55182

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-200983

github.com github.com/vercel-labs/fix-react2shell-next?tab=readme-ov-file

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2025-55182



Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.