Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0380

Kwetsbaarheden verholpen in React Server Components

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 05-12-2025
Revisie: 1.0.1

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

Het NCSC heeft middels een openbare bron vernomen dat misbruik van de kwetsbaarheid met kenmerk CVE-2025-55182 sinds 3 december is waargenomen. Inmiddels is er publieke proof-of-conceptcode beschikbaar voor de betreffende kwetsbaarheid, wat het risico op misbruik verhoogt.

Feiten

React heeft kwetsbaarheden verholpen in bepaalde versies van React Server Components (specifiek voor versies 19.0.0, 19.1.0, 19.1.1 en 19.2.0).

Duiding

Een ongeauthenticeerde aanvaller kan een malafide HTTP-verzoek sturen naar elke Server Function-endpoint dat, wanneer het door React wordt verwerkt, kan leiden tot remote code execution op de server. Echter, zelfs als een Server Function-endpoint niet is geïmplementeerd, kan exploitatie nog steeds mogelijk zijn via React Server Components. Door deze fout kunnen aanvallers op afstand willekeurige code uitvoeren, wat de integriteit van de getroffen applicaties ernstig in gevaar brengt.

De kwetsbaarheid bevindt zich in de React versies 19.0, 19.1.0, 19.1.1 en 19.2.0 van:

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

Als bovengenoemde pakketten worden gebruikt, upgrade dan onmiddellijk. Deze kwetsbaarheid is verholpen in de versies 19.0.1, 19.1.2 en 19.2.1. Als de React-code van uw applicatie geen server gebruikt, is uw applicatie niet gevoelig voor deze kwetsbaarheid. Eveneens, als uw applicatie geen framework, bundler of bundler-plugin gebruikt die React Server Components ondersteunt, is uw applicatie niet getroffen.

De volgende React-frameworks en bundlers zijn getroffen:

- Next
- React Router
- Waku
- @parcel/rsc
- @vitejs/plugin-rsc
- rwsdk

De kwetsbaarheid treft ook Next.js met App Router, en heeft hiervoor aanvankelijk het kenmerk CVE-2025-66478 toegewezen gekregen, maar is inmiddels als zelfstandig CVE-id teruggetrokken. De

kwetsbaarheid bevindt zich in de Next.js-versies 14.3.0-canary, 15.x en 16.x en is verholpen in de volgende gepatchte versies: 14.3.0-canary.88, 15.0.5, 15.1.9, 15.2.6, 15.3.6, 15.4.8, 15.5.7 en 16.0.7.

Update: Het NCSC heeft middels een openbare bron vernomen dat misbruik van de kwetsbaarheid met kenmerk CVE-2025-55182 sinds 3 december is waargenomen. Inmiddels is er publieke proof-of-conceptcode beschikbaar voor de betreffende kwetsbaarheid, wat het risico op grootschalig misbruik verhoogt.

Oplossingen

React heeft beveiligingsupdates uitgebracht om de kwetsbaarhedeid te verhelpen. Het NCSC adviseert om deze updates zo snel mogelijk te installeren. Zie de instructies van React voor meer informatie.

Dreigingsinformatie

Er is publieke PoC code beschrikbaar voor CVE-2025-55182 wat het risico op misbruik verhoogt.

Referenties

- https://aws.amazon.com/blogs/security/china-nexus-cyber-threat-groups-rapidly-exploit-react2shell-vulnerability-cve-2025-55182/
- https://nvd.nist.gov/vuln/detail/CVE-2025-55182
- https://nvd.nist.gov/vuln/detail/CVE-2025-66478
- https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components
- https://www.wiz.io/blog/critical-vulnerability-in-react-cve-2025-55182

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-55182	10.0 CRITICAL
CVE-2025-66478	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-502	Deserialization of Untrusted Data

Getroffen producten

Meta
react-server-dom-parcel
react-server-dom-turbopack
react-server-dom-webpack
Meta Open Source
react-server-dom-parcel
react-server-dom-turbopack
react-server-dom-webpack

Disclaimer