Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0394

Kwetsbaarheden verholpen in React Server Components

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-12-2025
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

De kwetsbaarheden zitten volgens het React team in onderstaande versies: - CVE-2025-55184 & CVE-2025-55183 - 19.0.0, 19.0.1 19.1.0, 19.1.1, 19.1.2, 19.2.0 and 19.2.1 - CVE-2025-67779 - 19.0.2, 19.1.3 and 19.2.2 De kwetsbaarheden worden in versies 19.0.3, 19.1.4, and 19.2.3 verholpen.

Feiten

Meta heeft kwetsbaarheden verholpen in React Server Components Parcel, Turbopack en Webpack.

Duiding

De kwetsbaarheden zijn gerelateerd aan onveilige deserialisatie van HTTP-verzoekpayloads, wat kan leiden tot Denial-of-Service-aanvallen en serverhangen. Dit heeft invloed op de beschikbaarheid van applicaties die gebruikmaken van deze versies. Daarnaast is er een informatielek dat kan resulteren in het blootleggen van de broncode van Server Functions onder specifieke omstandigheden. Deze kwetsbaarheden zijn kritiek voor server-side rendering in React-applicaties.

Oplossingen

Meta heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://react.dev/blog/2025/12/11/denial-of-service-and-source-code-exposure-in-react-server-components

- https://www.facebook.com/security/advisories/cve-2025-55183
- https://www.facebook.com/security/advisories/cve-2025-55184
- https://www.facebook.com/security/advisories/cve-2025-67779

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-67779	7.5 HIGH
CVE-2025-55183	5.3 MEDIUM

CVE-2025-55184	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-400	Uncontrolled Resource Consumption
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-502	Deserialization of Untrusted Data
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')

Getroffen producten

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

Disclaimer