GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA RÉPUBLIQUE DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPR 9108 Port-Vila, Vanuatu
Tél : (678) 33380

11 décembre 2025

Avis 114 : Vulnérabilité critique d'exécution de code à distance (RCE)

Date : 03 décembre 2025
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN par l'intermédiaire du CERT Vanuatu (CERTVU)), publie la présente alerte.

Cette alerte s'adresse aux organisations et administrateurs de système/réseau utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et administrateurs de système.

Objet de l'alerte

- CVE-2025-55182 (également appelée « React2Shell ») est une vulnérabilité critique d'exécution de code à distance (RCE) dans React Server Components (RSC).
- La vulnérabilité provient d'une désérialisation non sécurisée des charges utiles des requêtes HTTP entrantes dans le protocole « Flight » gérant RSC. Des charges utiles malformées ou malveillantes peuvent déclencher l'exécution de code arbitraire sur le serveur.

Systèmes concernés

• Composants React Server — plus précisément les modules react-server-dom-webpack, react-server-dom-parcel et react-server-dom-turbopack, dans les versions 19.0.0, 19.1.0, 19.1.1 et 19.2.0.

• Cadres et outils basés sur React RSC, notamment Next.js (versions 15.x et 16.x avec App Router) et d'autres regroupeurs/extensions compatibles avec RSC (par exemple, le plugin Vite RSC, le plugin Parcel RSC, RedwoodSDK, Waku, le mode React Router RSC).

Implication

Les attaquants peuvent exploiter cette vulnérabilité par les manières suivantes (vecteur d'attaque) :

- Un attaquant non authentifié envoie une requête HTTP spécialement conçue à un point de terminaison « Server Function » RSC.
- Comme le serveur traite/désérialise incorrectement les données de la requête, la charge utile contrôlée par l'attaquant déclenche l'exécution côté serveur d'un code JavaScript arbitraire, ce qui signifie l'exécution complète de code à distance sous les privilèges du serveur.

Mesures d'atténuation

Le CERTVU recommande les mesures suivantes :

Appliquez immédiatement le correctif

Mettez à jour les composants React Server Components vers les versions corrigées : react-server-dom- → version 19.0.1, 19.1.2 ou 19.2.1.

Références .

1. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-vulnerability-in-react-server-components-cve-2025-55182
2. https://www.cve.org/CVERecord?id=CVE-2025-55182