



DJ-CERT

Centre national de veille,
d'alerte et de réponse aux
attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 30-09-2026

BULLETIN ALERTES

Object	Vulnérabilité dans Next.js
Référence	1506
Date de Publication	2026-09-30
Sévérité	Critique

IMPACT :

Exécution de code à distance sur le serveur

SYSTÈME AFFECTÉ :

- Next.js versions 16.2.0 à antérieures à 16.3.6, utilisant l'implémentation Node.js de ImageResponse
- Next.js 15.x n'est pas vulnérable à cette exécution de code à distance

DÉSCRIPTION :

Une vulnérabilité critique a été corrigée dans la fonctionnalité ImageResponse du paquet next/og de Next.js, utilisée pour générer des images de prévisualisation (Open Graph). Elle provient d'un défaut d'échappement dans la bibliothèque tierce Satori, utilisée par Next.js pour convertir du JSX en SVG. Lorsqu'une application transmet des valeurs contrôlées par un utilisateur dans le contenu, les attributs ou les styles SVG traités par l'implémentation Node.js de ImageResponse, ces valeurs peuvent s'échapper de leur contexte et être interprétées comme du balisage SVG exécutable, conduisant à une exécution de code sur le serveur. L'implémentation Edge de ImageResponse n'est pas concernée.



SOLUTION :

Toute installation sur la branche 16.x, y compris 16.2.x, doit être mise à jour vers :

- Next.js 16.3.6 ou une version ultérieure (aucun correctif n'existe dans la branche 16.2.x elle-même)

DOCUMENTATION :

Bulletin de sécurité Next.js / Vercel :

- <https://nextjs.org/blog/nextjs-security-update-september-22-2026>
- <https://github.com/vercel/next.js/security/advisories/GHSA-vcvr-r3jv-pc5j>

CVE-2026-94545 :

- <https://www.cve.org/CVERecord?id=CVE-2026-94545>