DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 16-05-2026

BULLETIN ALERTES

Object	Vulnérabilité dans Next.js
Réference	1472
Date de Publication	2026-05-16
Sévérité	Elevé

IMPACT :

- **SSRF non authentifié** permettant d'accéder aux services internes, endpoints de métadonnées cloud (AWS, GCP, Azure) et API/panneaux d'administration
- **Risque d'exfiltration** d'identifiants cloud, clés API, secrets et configurations sensibles

SYSTÉME AFFECTÉ :

Next.js auto-hébergé (self-hosted) utilisant le serveur Node.js intégré :

- Versions 13.4.13 à 15.5.15
- Versions 16.0.0 à 16.2.4

DÉSCRIPTION :

Une vulnérabilité de type Server-Side Request Forgery (SSRF) a été découverte dans Next.js. La faille réside dans le gestionnaire des requêtes WebSocket Upgrade du serveur Node.js intégré de Next.js. En envoyant une requête HTTP spécialement conçue au format absolu avec l'en-tête « Upgrade : websocket », un attaquant non authentifié peut forcer le serveur Next.js à effectuer des requêtes HTTP internes vers n'importe quel hôte accessible depuis le serveur sur le port 80. L'exploitation réussie peut entraîner la divulgation des identifiants cloud, clés API, secrets et données de configuration sensibles.

SOLUTION :

1. Mettre à jour immédiatement Next.js vers la version **15.5.16** ou **16.2.5** (correctifs publiés par Vercel le 11 mai 2026).

2. Si la mise à jour est impossible, bloquer toutes les requêtes WebSocket Upgrade au niveau du reverse proxy ou du load balancer si l'application ne les utilise pas activement.

3. Restreindre le trafic sortant du serveur d'origine en bloquant l'accès aux services de métadonnées cloud internes (169.254.169.254, metadata.google.internal) et aux réseaux internes non liés à l'application.

4. Ne pas exposer directement les serveurs d'origine Next.js à Internet ; toujours utiliser un reverse proxy avec validation stricte des en-têtes.

5. Sur AWS, basculer vers IMDSv2 (qui n'est pas exploitable par cette SSRF de type GET) afin de protéger les identifiants des instances EC2.

6. Auditer les logs pour détecter d'éventuelles tentatives d'exploitation (requêtes HTTP avec en-tête Upgrade: websocket non sollicitées).

DOCUMENTATION :

CVE-2026-44578

- https://nvd.nist.gov/vuln/detail/CVE-2026-44578