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

Autorité Nationale de Cybersécurité

Djibouti le, 19-05-2026

BULLETIN ALERTES

Object	Vulnérabilité critique dans NGINX
Réference	1475
Date de Publication	2026-05-19
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance
- Déni de Service (DoS)

SYSTÉME AFFECTÉ :

- **NGINX Open Source** : Versions **0.6.27 à 1.30.0** (inclus)
- **NGINX Plus** : Versions **R32 à R36**
- Impacte également : NGINX Ingress Controller, F5 WAF, et tout produit basé sur ce module.

DÉSCRIPTION :

CVE-2026-42945 est une vulnérabilité critique de type Heap Buffer Overflow dans le module ngx_http_rewrite_module de NGINX. Elle permet à un attaquant non authentifié d'envoyer une seule requête HTTP spécialement conçue pour provoquer un débordement de tampon sur la heap du processus worker.

L'attaque consiste à cibler des règles de rewrite vulnérables contenant des captures PCRE non nommées ($1, $2, etc.) associées à un point d'interrogation (?) dans la chaîne de remplacement. Lors du traitement de la requête, NGINX alloue un buffer sur la heap pour construire la nouvelle URI. Une erreur de calcul de taille provoque alors un Heap Buffer Overflow, entraînant soit le crash immédiat du worker (déni de service), soit, dans des scénarios avancés avec heap grooming, une exécution de code arbitraire à distance. L'attaque est entièrement non authentifiée et ne nécessite qu'une seule requête.

NB : cette vulnérabilité est activement exploitée.

SOLUTION :

Mettre à jour immédiatement vers :

- NGINX Open Source **1.30.1** ou **1.31.0**
- NGINX Plus : version corrigée (R37 ou patch officiel)

DOCUMENTATION :

• NVD — CVE-2026-42945 — https://nvd.nist.gov/vuln/detail/CVE-2026-42945

• Analyse technique (depthfirst / NGINX Rift) — https://www.picussecurity.com/resource/blog/nginx-rift-cve-2026-42945-critical-heap-buffer-overflow-vulnerability-explained

• VulnCheck — Confirmation exploitation active — https://vulncheck.com/blog/cve-2026-42945-nginx-rift