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

Autorité Nationale de Cybersécurité

Djibouti le, 16-07-2026

BULLETIN ALERTES

Object	Vulnérabilité dans NGINX
Réference	1494
Date de Publication	2026-07-16
Sévérité	Moyen

IMPACT :

- Déni de service
- Corruption limitée de la mémoire du processus worker

SYSTÉME AFFECTÉ :

- NGINX Open Source versions 0.8.11 à 1.30.3
- NGINX Open Source versions 1.31.2 (branche mainline)
- NGINX Plus PLS.37.0.0.1 versions antérieures à PLS.37.0.3.1
- NGINX Plus R36 versions antérieures à R36 P7
- NGINX Plus R33

DÉSCRIPTION :

Une vulnérabilité a été corrigée dans NGINX Plus et NGINX Open Source. Son exploitation pourrait permettre à un attaquant de provoquer une corruption limitée de la mémoire du processus *worker* ou un déni de service.

SOLUTION :

Mettre à jour NGINX Open Source et NGINX Plus vers les versions corrigées suivantes :

- **NGINX Open Source (branche stable)** : 1.30.4 ou une version ultérieure
- **NGINX Open Source (branche mainline)** : 1.31.3 ou une version ultérieure
- **NGINX Plus PLS.37.0.0.1** : PLS.37.0.3.1 ou une version ultérieure
- **NGINX Plus R36** : R36 P7 ou une version ultérieure

Pour les déploiements utilisant **NGINX Plus R33**, se référer à l'avis de sécurité **F5 K000162098** afin de déterminer la version de mise à niveau ou les recommandations applicables à cette branche.

DOCUMENTATION :

Bulletin de sécurité NGINX (F5)

- https://my.f5.com/manage/s/article/K000162098

CVE-2026-56434 :

- https://www.cve.org/CVERecord?id=CVE-2026-56434