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

Autorité Nationale de Cybersécurité

Djibouti le, 22-11-2026

BULLETIN ALERTES

Object	Vulnérabilité dans le module HTTP/2 de NGINX (ngx_http_v2_module)
Réference	1517
Date de Publication	2026-11-18
Sévérité	Critique

IMPACT :

- Exécution de code à distance (RCE) non authentifiée (sous conditions)
- Corruption de la mémoire (heap buffer overflow)
- Interruption de service (crash des processus workers NGINX)

SYSTÉME AFFECTÉ :

- NGINX Open Source versions 1.9.5 à 1.30.6 et 1.31.0 à 1.31.8, lorsque le protocole HTTP/2 est activé
- NGINX Plus versions concernées (branches 37.0.x avant 37.0.8.1 et 37.1.x/37.2.x avant 37.3.0.1, ainsi que R34 à R36)
- Configurations utilisant le module ngx_http_v2_module avec HTTP/2 activé (y compris serveurs servant uniquement du contenu statique)

DÉSCRIPTION :

Une vulnérabilité d'integer underflow (CWE-191) a été identifiée dans la gestion du contrôle de flux
HTTP/2 du module ngx_http_v2_module de NGINX. Lors du traitement de certains trafics HTTP/2, la
fenêtre de contrôle de flux peut dépasser les limites autorisées, entraînant un débordement de tampon
sur le tas (heap buffer overflow, CWE-787). Un attaquant distant non authentifié peut ainsi provoquer
un crash des processus workers NGINX (déni de service) ou, lorsque les mécanismes de protection
mémoire (notamment ASLR) sont absents ou contournés, une exécution de code avec les privilèges du
processus worker NGINX. La vulnérabilité est présente depuis l'introduction du support HTTP/2 dans
NGINX 1.9.5 (2015). Des preuves de concept publiques existent et des démonstrations de RCE en
laboratoire ont été publiées. Aucune exploitation active à grande échelle n'est confirmée par les sources
officielles consultées à la date de ce bulletin.

SOLUTION :

Mettre à jour NGINX Open Source vers la version 1.30.7 (branche stable) ou 1.31.9 (branche mainline), publiées le 18/11/2026.
Pour NGINX Plus, appliquer les versions corrigées 37.0.8.1 ou 37.3.0.1 selon la branche utilisée.

Sous les distributions Linux (notamment Red Hat Enterprise Linux 9 et 10), installer les paquets nginx mis à jour via les errata de sécurité correspondants (ex. RHSA-2026:100744 et suivants). Redémarrer le service nginx après la mise à jour.

En l’absence d’application immédiate du correctif, désactiver temporairement HTTP/2 (directive http2 off; ou suppression du paramètre http2 des directives listen) constitue une mesure de mitigation. Cette mesure peut impacter les clients gRPC ou d’autres usages dépendant d’HTTP/2.

DOCUMENTATION :

Avis de sécurité F5 / NGINX et Red Hat

- my.f5.com/manage/s/article/K000163926
- nginx.org/news.html
- access.redhat.com/security/cve/CVE-2026-123007
- access.redhat.com/security/vulnerabilities/RHSB-2026-019

CVE-2026-123007 :

- cve.org/CVERecord