AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SÉCURITÉ

nginx2root : exécution de code à distance dans NGINX via HTTP/2

Sommaire

I. Contexte 3
II. Description des vulnérabilités 3
Versions affectées et corrigées 4
III. Vecteur d'attaque 5
IV. État de l'exploitation 6
V. Exposition en Afrique et au Cameroun 6
VI. Conclusion et actions recommandées....6
VII. Références 7

I. Contexte

Le 18 novembre 2026, F5 a publié, hors cycle, des correctifs pour cinq vulnérabilités critiques affectant NGINX, le serveur web et proxy inverse le plus utilisé au monde. La plus grave, référencée CVE-2026-123007 et surnommée « nginx2root », réside dans le module HTTP/2 et existe depuis plus de onze ans : elle touche toutes les versions publiées depuis la 1.9.5 (septembre 2015).

F5 attribue aux cinq failles un score CVSS v4.0 de 9.2 (critique). Elles permettent à un attaquant non authentifié d'exécuter du code sur le serveur avec les privilèges des processus de travail (workers) de NGINX. Les cinq failles ont été découvertes par l'équipe de recherche Xint (Theori) ; la principale, CVE-2026-123007, a aussi été signalée séparément par Wiz Research, Rapid7 et Ikotas Labs. Les équipes de Wiz, Xint et Rapid7 ont démontré l'exploitation de cette dernière, et le CIRCL luxembourgeois a publié des recommandations de réponse.

II. Description des vulnérabilités

La vulnérabilité principale, nginx2root, est une corruption de mémoire dans le contrôle de flux du protocole HTTP/2 : un dépassement d'entier (integer overflow) dans la gestion des fenêtres d'émission conduit à une lecture et à une écriture hors limites sur le tas. Quatre autres failles, de type utilisation après libération (use-after-free) et corrigées simultanément, touchent des configurations plus spécifiques de NGINX. Le projet NGINX utilise sa propre échelle de

gravité, distincte du score CVSS de F5 : il y classe CVE-2026-123007 et CVE-2026-113425 au niveau « major » et les trois autres au niveau « medium ».

CVE	Condition d'exploitation	Score CVSS v4.0
CVE-2026-123007 (nginx2root)	HTTP/2 activé (versions 1.9.5 à 1.31.8)	9.2 Critique
CVE-2026-123633	HTTP/2 activé, requêtes relayées vers un serveur amont alors que le worker manque de connexions disponibles (worker_connections) ; versions 1.19.7 à 1.31.8	9.2 Critique
CVE-2026-123634	Résolveur DNS configuré et nom du serveur amont construit à partir de variables, avec une sous-requête SSI ou mirror ; versions 0.6.18 à 1.31.8	9.2 Critique
CVE-2026-121810	HTTP/3 activé, requêtes relayées vers un serveur amont ; versions 1.25.0 à 1.31.8	9.2 Critique
CVE-2026-113425	NGINX utilisé comme proxy de messagerie avec auth_http ; versions 0.5.33 à 1.31.8	9.2 Critique

Alias	nginx2root (CVE-2026-123007)
Produit	NGINX Open Source et NGINX Plus
Type	Corruption de mémoire (dépassement d'entier) dans le contrôle de flux HTTP/2
Impact	Exécution de code arbitraire à distance sans authentification
Score CVSS v4.0	**9.2 Critique (évaluation de F5)**
État de l'exploitation	**Code d'exploitation publié par Rapid7 ; aucune attaque réelle signalée au 19 novembre 2026**
Découverte par	Xint (Theori) ; signalée séparément par Wiz Research, Rapid7 et Ikotas Labs
Date de divulgation	18 novembre 2026
Correctif	NGINX 1.31.9 et 1.30.7, NGINX Plus 37.3.0.1 et 37.0.8.1

Versions affectées et corrigées

Les versions suivantes sont affectées. À la date de rédaction (19 novembre 2026), Ubuntu (16.04 à 26.10), Debian (bookworm, trixie, forky), Red Hat Enterprise Linux, SUSE et Amazon Linux 2 n'avaient pas encore publié de paquet corrigé ; des paquets corrigés étaient disponibles pour Alpine 3.24, AlmaLinux et Amazon Linux 2023. Les distributions rétroportent les

correctifs sans modifier le numéro de version : se référer au suivi de sécurité de chaque distribution.

Produit	Versions affectées	Versions corrigées
NGINX Open Source (mainline)	1.31.0 à 1.31.8	1.31.9 ou ultérieure
NGINX Open Source (stable et branches antérieures)	1.9.5 à 1.30.6	1.30.7 ou ultérieure
NGINX Plus 37.1 à 37.2	37.1.0 à 37.2.0.1	37.3.0.1 ou ultérieure
NGINX Plus 37.0	37.0.0 à 37.0.7.1	37.0.8.1 ou ultérieure
NGINX Plus R34 à R36	Toutes	Aucun correctif : migrer vers une version 37.x corrigée
Images Docker officielles	Antérieures aux correctifs	Tags 1.31.9 et 1.30.7 (y compris Alpine) ; télécharger de nouveau les tags latest, mainline et stable et reconstruire les images dérivées

III. Vecteur d'attaque

L'exploitation de nginx2root se déroule comme suit :

- L'attaquant ouvre une connexion HTTP/2 vers un serveur NGINX exposé, sans aucune authentification.
- Il envoie un volume important de trames HTTP/2 spécialement conçues qui faussent le calcul des fenêtres de contrôle de flux et provoquent une corruption de la mémoire du processus worker.
- Il obtient l'exécution de code avec les privilèges du worker NGINX, ce qui lui permet d'intercepter le trafic, de voler les certificats et les secrets, ou de rebondir vers les serveurs amont.
- En combinant cette faille avec une vulnérabilité distincte du noyau Linux (module SCTP), non corrigée à ce jour, les chercheurs de Xint ont obtenu les privilèges root sur l'hôte, y compris depuis un conteneur Docker.

L'attaque nécessite de contourner la protection ASLR, ce que Wiz et Xint ont réussi lors de leurs tests. Le code d'exploitation de Rapid7 dépend en outre d'une routine de copie mémoire de la glibc propre aux systèmes x86-64 et nécessite environ 128 Go de trafic HTTP/2 sur une seule connexion : sa démonstration a duré 2 minutes 30 secondes, et l'attaque échoue sur les liaisons trop lentes. L'attaque de Xint a fonctionné contre des serveurs de test hébergés chez AWS, GCP et Azure via des adresses IP publiques.

IV. État de l'exploitation

Au 19 novembre 2026, ni F5, ni Wiz, ni Rapid7, ni Xint ne signalent d'attaque réelle, et aucune des cinq failles ne figure au catalogue des vulnérabilités exploitées connues (KEV) de la CISA. Un code d'exploitation est toutefois public : Rapid7 a publié le sien sur GitHub pour CVE-2026-123007, même s'il ne fonctionne en l'état que dans des conditions de laboratoire. Xint et Wiz, dont les attaques ont réussi contre des serveurs réels, ne publient pas les leurs. De faux dépôts se présentant comme des codes d'exploitation circulent également et sont à éviter.

La publication du code de Rapid7 et la démonstration, par Xint, d'attaques réussies contre des serveurs en nuage exposés sur Internet rendent probable l'apparition rapide de codes d'exploitation plus fiables. Les serveurs NGINX constituent une cible privilégiée en raison de leur position en frontal de très nombreux services.

V. Exposition en Afrique et au Cameroun

NGINX est massivement déployé au Cameroun et en Afrique comme serveur web, proxy inverse, répartiteur de charge et passerelle d'API. Il est placé en frontal des portails des administrations, des plateformes bancaires et de paiement mobile, des services des opérateurs de télécommunications et de nombreux sites hébergés localement ou en nuage (cloud).

HTTP/2 est activé dans la grande majorité des configurations HTTPS récentes. Par ailleurs, de nombreux serveurs fonctionnent avec des paquets de distribution Linux qui n'étaient pas encore corrigés à la date de rédaction, ou avec des versions anciennes jamais mises à jour, ce qui accroît fortement la surface d'exposition nationale. Aucune mesure publique du nombre de serveurs vulnérables au Cameroun n'est disponible à ce jour.

VI. Conclusion et actions recommandées

nginx2root est une vulnérabilité critique qui permet la compromission à distance de serveurs NGINX sans authentification. Le CIRT recommande vivement les actions suivantes :

1. Recenser tous les serveurs NGINX, y compris les images Docker, les contrôleurs Ingress Kubernetes et les équipements embarquant NGINX, et relever leur version.
2. Mettre à jour sans délai vers NGINX 1.31.9 ou 1.30.7, ou NGINX Plus 37.3.0.1 ou 37.0.8.1, puis redémarrer complètement le service : un simple rechargement (reload) ne remplace pas le binaire en cours d'exécution et laisse les anciens processus worker actifs. Pour les paquets NGINX fournis par les distributions Linux, appliquer le paquet corrigé dès sa publication et, dans l'intervalle, appliquer la mesure 3.
3. En attendant la mise à jour, désactiver temporairement HTTP/2 : à partir de la version 1.25.1, ajouter la directive « http2 off; » et retirer le paramètre http2 des

directives listen ; pour les versions antérieures, retirer le paramètre http2 des directives listen. Vérifier ensuite avec openssl s_client que le protocole h2 n'est plus négocié. Cette mesure ne protège que contre les deux failles HTTP/2 (CVE-2026-123007 et CVE-2026-123633), pas contre les trois autres.

4. Désactiver HTTP/3 lorsqu'il n'est pas indispensable, remplacer les noms de serveurs amont construits à partir de variables par des groupes upstream fixes, désactiver la directive mirror lorsqu'elle n'est pas nécessaire, et restreindre le proxy de messagerie à l'interface locale ou aux réseaux de confiance.
5. Lorsque le protocole SCTP n'est pas utilisé, bloquer le chargement du module correspondant (ajout de « install sctp /bin/false » dans un fichier .conf de /etc/modprobe.d/), la faille du noyau n'étant pas encore corrigée. Cette mesure ne décharge pas un module déjà chargé.
6. Surveiller les processus inattendus lancés par les workers NGINX, les arrêts anormaux ou les fichiers d'image mémoire (core dump), les connexions HTTP/2 longues à fort trafic entrant mais avec peu de requêtes journalisées, ainsi que les connexions sortantes inhabituelles.
7. Garder à l'esprit qu'un journal d'accès sans anomalie ne permet pas d'exclure une attaque, et signaler tout incident suspect au CIRT.

Pour tout incident ou toute demande d'assistance, contactez le CIRT par ses canaux habituels.

VII. Références

- NGINX (projet officiel), annonces de sécurité : https://nginx.org/en/security_advisories.html
- NGINX, journal des modifications de la version 1.30.7 : https://nginx.org/en/CHANGES-1.30
- F5, avis K000163926 relatif à CVE-2026-123007 : https://my.f5.com/manage/s/article/K000163926
- F5, notification de sécurité hors cycle du 18 novembre 2026 (K000164058) : https://my.f5.com/manage/s/article/K000164058
- NIST, National Vulnerability Database (NVD) : https://nvd.nist.gov/vuln/detail/CVE-2026-123007
- MITRE, programme CVE : https://www.cve.org/CVERecord?id=CVE-2026-123007
- CIRCL, Vulnerability Lookup : https://vulnerability.circl.lu/vuln/CVE-2026-123007
- Red Hat, fiche CVE : https://access.redhat.com/security/cve/cve-2026-123007
- Ubuntu, suivi de sécurité : https://ubuntu.com/security/CVE-2026-123007
- Debian, suivi de sécurité : https://security-tracker.debian.org/tracker/CVE-2026-123007
- Xint, rapport de recherche nginx2root : https://xint.io/blog/nginx2root-remote-code-execution
- Wiz Research, vulnérabilités RCE HTTP/2 de NGINX : https://www.wiz.io/blog/nginx-http2-rce-vulnerabilities
- Tenable, FAQ nginx2root : https://www.tenable.com/blog/nginx2root-cve-2026-123007-frequently-asked-questions-about-five-critical-nginx
- Sophos, avis de sécurité nginx2root : https://www.sophos.com/en-us/security-advisories/sophos-sa-20261118-nginx2root
- The Hacker News, 18 novembre 2026 : https://thehackernews.com/2026/11/10-year-old-nginx-http2-flaw-lets.html