AVIS DE SECURITE

Objet	**Multiples vulnérabilités dans les produits F5 NGINX**
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-265
TLP	WHITE

Résumé

F5 a publié le 14/10/2026 des correctifs pour plusieurs vulnérabilités affectant NGINX Open Source, NGINX Plus, NGINX Ingress Controller, NGINX Gateway Fabric, NGINX Instance Manager, F5 WAF for NGINX et F5 DoS for NGINX. Les plus sévères (CVSS v3.1 jusqu'à 8.8) permettent l'injection de directives dans la configuration (CVE-2026-91184) ou, via des débordements de tas et une utilisation après libération (CVE-2026-15176, 93479, 97205 : 8.1), le plantage de processus et potentiellement l'exécution de code à distance. Aucune exploitation n'est signalée.

Risque de sécurité

- Exécution de code arbitraire à distance
- Déni de service à distance
- Contournement de la politique de sécurité (authentification externe, vérification des certificats clients)
- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données

Systèmes affectés

- F5 NGINX Open Source 1.x antérieures à 1.31.7
- F5 NGINX Plus 37.x antérieures à 37.2.0
- NGINX Ingress Controller 5.x antérieures à 5.7.0
- NGINX Gateway Fabric 2.x antérieures à 2.8.0
- NGINX Instance Manager 2.x antérieures à 2.24.0
- F5 WAF for NGINX 5.x antérieures à 5.16.0
- F5 DoS for NGINX 4.x antérieures à 4.11.0

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 14/10/2026 :
   - https://my.f5.com/manage/s/article/K000162416
   - https://my.f5.com/manage/s/article/K000162606
   - https://my.f5.com/manage/s/article/K000162607
   - https://my.f5.com/manage/s/article/K000162608
   - https://my.f5.com/manage/s/article/K000162613
2. Mettre à jour les produits NGINX concernés vers les versions corrigées indiquées dans les bulletins F5