ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits F5
Numéro de Référence	60810602/26
Date de Publication	06 Février 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- BIG-IP Advanced WAF/ASM version antérieure à 17.1.3 ;
- NGINX Plus version antérieure à R36 P2, R35 P1, R32 P4 ;
- NGINX Open Source version antérieure à 1.29.5 et 1.28.2 ;
- NGINX Ingress Controller version 5.3.0 à 5.3.2, 4.0.0 à 4.0.1, 3.4.0 à 3.7.1 ;
- NGINX Gateway Fabric version 2.0.0 à 2.4.0, 1.2.0 à 1.6.2 ;
- NGINX Instance Manager version 2.15.1 à 2.21.0 ;
- BIG-IP Container Ingress Services for Kubernetes and OpenShift version antérieure à 2.20.2, 2.20.1 avec Helm version 0.0.363 ;
- BIG-IP APM version antérieure à 17.1.3.1 ;
- APM Clients version antérieure à 7.2.6.2 ;
- BIG-IP (all modules) version antérieure à 17.5.1.4, 17.1.3.1, 21.0.0.1 ;

Identificateurs externes

- CVE-2025-58120, CVE-2025-53474, CVE-2025-60016, CVE-2025-53868,
- CVE-2025-54854, CVE-2025-41430, CVE-2025-55670, CVE-2025-60013,
- CVE-2025-61935,

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits F5 susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de causer un déni de service, d'exécuter du code arbitraire à distance et de porter atteinte à la confidentialité des données.

Solution

Veuillez se référer au bulletin de sécurité F5 du 04 Février 2026 pour plus d'information.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risque

- Déni de service ;
- Exécution du code arbitraire à distance ;
- Atteinte à la confidentialité des données ;

Annexe

Bulletin de sécurité F5 du 04 Février 2026 :

- https://my.f5.com/manage/s/article/K000159076