



BULLETIN DE SECURITE

Titre	Vulnérabilité dans les produits F5
Numéro de Référence	50640811/24
Date de Publication	08 Novembre 2024
Risque	Important
Impact	Important

Systemes affectés

- NGINX API Connectivity Manager versions 1.x postérieures à 1.3.0 et antérieures à 1.9.3
- NGINX Ingress Controller versions antérieures à 3.7.1
- NGINX Instance Manager versions 2.x postérieures à 2.5.0 et antérieures à 2.17.4
- NGINX Plus toutes versions

Identificateurs externes

- CVE-2024-10318

Bilan de la vulnérabilité

Une vulnérabilité a été corrigée dans les versions susmentionnées de F5. L'exploitation de cette faille peut permettre à un attaquant de contourner la politique de sécurité.

Solution

Veillez se référer au bulletin de sécurité F5 du 06 novembre 2024 pour plus d'information.

Risque

- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité F5 du 06 novembre 2024:

- <https://my.f5.com/manage/s/article/K000148232>