



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits F5
Numéro de Référence	60081501/26
Date de publication	16 Janvier 2026
Risque	Important
Impact	Important

Systèmes affectés

- BIG-IP (DNS, Link Controller) versions 15.1.0 - 15.1.10
- BIG-IP (DNS, Link Controller) versions 16.1.0 - 16.1.6
- BIG-IP (DNS, Link Controller) versions 17.1.0 - 17.1.3
- BIG-IP (DNS, Link Controller) versions 17.5.0 - 17.5.1
- BIG-IP (DNS, Link Controller) versions 21.0.0
- F5OS-A versions 1.5.1 - 1.5.4
- F5OS-A versions 1.8.0 - 1.8.3
- F5OS-C versions 1.6.0 - 1.6.4
- F5OS-C versions 1.8.0 - 1.8.2

Identificateurs externes

- CVE-2024-5642 CVE-2025-40778 CVE-2025-8677

Bilan de la vulnérabilité

F5 Networks annonce la correction de trois vulnérabilités affectant ses produits susmentionnés. Un attaquant distant peut exploiter ces vulnérabilités pour accéder à des données confidentielles ou causer un déni de service.

Solution

Veillez se référer au bulletin de sécurité F5 Networks afin d'installer les nouvelles mises à jour.

Risque

- Accès à des données confidentielles
- Dénier de service

Référence

Bulletin de sécurité F5 networks:

- <https://my.f5.com/manage/s/article/K000157317>
- <https://my.f5.com/manage/s/article/K000157334>
- <https://my.f5.com/manage/s/article/K000159546>