



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits F5
Numéro de Référence	57571610/25
Date de Publication	16 Octobre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- BIG-IP Next pour Kubernetes Versions 2.x antérieure à 2.1.0
- BIG-IP Next CNF Versions 2.x antérieure à 2.0.1
- BIG-IP Next CNF Versions 1.1.0 à 1.4.1
- BIG-IP Next SPK Versions 1.x antérieure à 1.7.14 EHF-2
- BIG-IP Next SPK Versions 2.x antérieure à 2.0.1
- BIG-IP Advanced WAF/ASM versions 17.x, 16.x et 15.x
- BIG-IP (all modules) versions 17.x, 16.x et 15.x
- BIG-IP SSL Orchestrator 17.x, 16.x et 15.x
- F5OS-A Versions 1.x antérieure à 1.8.3 et 1.5.4

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 15 Octobre 2025 pour plus d'information.

Risque

- Déni de service

- Exécution du code arbitraire à distance
- Atteinte à la confidentialité des données

Annexe

Bulletin de sécurité F5 du 15 Octobre 2025:

- <https://my.f5.com/manage/s/article/K000156623>
- <https://my.f5.com/manage/s/article/K44517780>
- <https://my.f5.com/manage/s/article/K000139514>
- <https://my.f5.com/manage/s/article/K000151902>
- <https://my.f5.com/manage/s/article/K000156602>
- <https://my.f5.com/manage/s/article/K000150667>
- <https://my.f5.com/manage/s/article/K000154614>
- <https://my.f5.com/manage/s/article/K000154661>