DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 21-08-2025

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits F5
Réference	1379
Date de Publication	2025-08-19
Sévérité	Elevé

IMPACT :

- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service à distance
- Non spécifié par l'éditeur
- Élévation de privilèges

SYSTÉME AFFECTÉ :

- BIG-IP (APM) versions 16.1.x antérieures à 16.1.6
- BIG-IP (APM) versions 17.1.x antérieures à 17.1.2.2
- BIG-IP (APM) versions 17.5.0 à 17.5.1, 17.1.0 à 17.1.2, 16.1.0 à 16.1.6 et 15.1.0 à 15.1.10
- BIG-IP (tous les modules) versions 16.1.0 à 16.1.5 antérieures à 16.1.6
- BIG-IP (tous les modules) versions 16.1.x antérieures à Hotfix-BIGIP-16.1.6.0.27.3-ENG.iso3
- BIG-IP (tous les modules) versions 17.1.0 à 17.1.2 antérieures à 17.1.2.2
- BIG-IP (tous les modules) versions 17.1.x antérieures à Hotfix-BIGIP-17.1.2.2.0.259.12-ENG.iso3
- BIG-IP (tous les modules) versions 17.5.x antérieures à Hotfix-BIGIP-17.5.1.0.80.7-ENG.iso3
- BIG-IP (tous les modules) versions 17.x antérieures à 17.1.0 - 17.1.2
- BIG-IP Next (tous les modules) versions 20.3.0
- BIG-IP Next (tous les modules) versions 20.x antérieures à 20.3.0
- BIG-IP Next CNF versions 2.0.0 à 2.0.2 et 1.1.0 à 1.4.1
- BIG-IP Next CNF versions 2.x antérieures à 2.0.0 - 2.0.2
- BIG-IP Next for Kubernetes versions 2.0.0
- BIG-IP Next for Kubernetes versions 2.x antérieures à 2.0.0
- BIG-IP Next SPK versions 2.0.0 à 2.0.2 et 1.7.0 à 1.9.2
- BIG-IP Next SPK versions 2.0.x antérieures à 2.0.2
- NGINX Open Source versions 0.7.22 à 1.29.0 antérieures à 1.29.1
- NGINX Plus versions antérieures à R32 P3
- NGINX Plus versions antérieures à R35
- NGINX Plus versions R33 antérieures à R33 P3
- NGINX Plus versions R34 antérieures à R34 P2

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans les produits F5. Certaines peuvent être exploitées par un attaquant pour obtenir une élévation de privilèges, provoquer un déni de service à distance ou compromettre la confidentialité des données.

SOLUTION :

Consultez le bulletin de sécurité de l'éditeur pour obtenir les correctifs (cf. section Documentation).

DOCUMENTATION :

- Bulletin de sécurité F5 K000141436 du 13 août 2025

https://my.f5.com/manage/s/article/K000141436

- Bulletin de sécurité F5 K000151546 du 13 août 2025

https://my.f5.com/manage/s/article/K000151546

- Bulletin de sécurité F5 K000151782 du 13 août 2025

https://my.f5.com/manage/s/article/K000151782

- Bulletin de sécurité F5 K000152001 du 13 août 2025

https://my.f5.com/manage/s/article/K000152001

- Bulletin de sécurité F5 K000152049 du 13 août 2025

https://my.f5.com/manage/s/article/K000152049

- Bulletin de sécurité F5 K000152635 du 13 août 2025

https://my.f5.com/manage/s/article/K000152635

- Référence CVE CVE-2025-46405

https://www.cve.org/CVERecord?id=CVE-2025-46405

- Référence CVE CVE-2025-48500

https://www.cve.org/CVERecord?id=CVE-2025-48500

- Référence CVE CVE-2025-52585

https://www.cve.org/CVERecord?id=CVE-2025-52585

- Référence CVE CVE-2025-53859

https://www.cve.org/CVERecord?id=CVE-2025-53859

- Référence CVE CVE-2025-54500

https://www.cve.org/CVERecord?id=CVE-2025-54500

- Référence CVE CVE-2025-54809

https://www.cve.org/CVERecord?id=CVE-2025-54809