



BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits F5
Numéro de Référence	40080302/23
Date de Publication	03 Février 2023
Risque	Important
Impact	Important

Systemes affectés

- F5 BIG-IP (tous modules) versions 17.0.0.x antérieures à 17.0.0.2
- F5 BIG-IP (tous modules) versions 16.1.x antérieures à 16.1.3.3
- F5 BIG-IP (tous modules) versions 15.1.x antérieures à 15.1.8.1
- F5 BIG-IP (tous modules) versions 14.1.x antérieures à 14.1.5.3
- BIG-IP APM Clients versions 7.2.x antérieures à 7.2.31
- BIG-IP SPK version 1.6.0

Identificateurs externes

- CVE-2023-22374 , CVE-2023-22358 , CVE-2023-22842 , CVE-2023-22323 , CVE-2023-22281 , CVE-2023-22341 , CVE-2023-22664 , CVE-2023-22340 , CVE-2023-23552 , CVE-2023-22839 , CVE-2023-23555 , CVE-2023-22657 , CVE-2023-22422 , CVE-2023-22283 , CVE-2023-22418 , CVE-2023-22302 , CVE-2023-22326

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits F5 susmentionnés. Un attaquant pourrait exploiter ces failles afin d'exécuter du code arbitraire à distance, causer un déni de service, contourner la politique de sécurité ou porter atteinte à la confidentialité de données.

Solution

F5 confirme qu'aucun correctif n'est publié pour la vulnérabilité « CVE-2023-22374 », permettant à un attaquant authentifié de causer un déni de service et d'exécuter du code arbitraire à distance. Toutefois des mesures de contournement sont disponibles.

Veuillez se référer au bulletin de sécurité F5 du 01 Février 2023 pour plus d'information.

Risque

- Exécution de code arbitraire à distance
- Dénî de service
- Contournement de la politique de sécurité
- Atteinte à la confidentialité de données

Annexe

Bulletins de sécurité F5 du 01 Février 2023:

- <https://my.f5.com/manage/s/article/K000130496>