



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant F5 BIG-IP
Numéro de Référence	28181812/20
Date de publication	18 Décembre 2020
Risque	Important
Impact	Important

Systemes affectés

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) versions 16.x antérieures à 16.0.1.1
- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, FPS, Link Controller, PEM) versions 15.x antérieures à 15.1.1
- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) versions 14.x antérieures à 14.1.3.1
- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) versions 13.x antérieures à 13.1.3.5
- BIG-IP (Advanced WAF) versions 16.x antérieures à 16.0.1.1
- BIG-IP (Advanced WAF) versions 15.x antérieures à 15.1.1
- BIG-IP (Advanced WAF) versions 14.x antérieures à 14.1.3.1
- BIG-IP (Advanced WAF) versions 13.x antérieures à 13.1.3.5
- BIG-IP (LTM/CGNAT) versions 16.x antérieures à 16.0.1
- BIG-IP (LTM/CGNAT) versions 15.x antérieures à 15.1.1
- BIG-IP (LTM/CGNAT) versions 14.x antérieures à 14.1.3.1
- BIG-IP (DNS, GTM) versions 15.x antérieures à 15.1.2

Identificateurs externes

CVE-2020-27727 CVE-2020-27718 CVE-2020-27715 CVE-2020-27716 CVE-2020-27720
CVE-2020-27723 CVE-2020-27717 CVE-2020-27721 CVE-2020-27728

Bilan de la vulnérabilité

F5 Networks annonce la correction de plusieurs vulnérabilités affectant plusieurs versions de sa famille de produits BIG-IP. Un attaquant distant peut exploiter ces vulnérabilités pour causer un déni de service ou d'accéder à des données confidentielles.

Solution

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

Risques

- Déni de service
- Accès à des données confidentielles

Références

Bulletins de sécurité F5 networks:

- <https://support.f5.com/csp/article/K50343630>
- <https://support.f5.com/csp/article/K73657294>
- <https://support.f5.com/csp/article/K58102101>
- <https://support.f5.com/csp/article/K25691186>
- <https://support.f5.com/csp/article/K51574311>
- <https://support.f5.com/csp/article/K04048104>
- <https://support.f5.com/csp/article/K42933418>
- <https://support.f5.com/csp/article/K43850230>
- <https://support.f5.com/csp/article/K52035247>
- <https://support.f5.com/csp/article/K45143221>