NEWSCAST CYBER THREAT INTELLIGENCE

CVE-2022-1388 F5 BIG-IP

CERT ADVENS

12/05/2022 / TLP-WHITE

SOMMAIRE

01 F5 BIG-IP CVE-2022-1388

01.1 RESUME

Le 4 mai 2022, l'entreprise F5 a publié le bulletin K23605346 à propos de la CVE-2022-1388 : Il s'agit d'une vulnérabilité critique qui affecte plusieurs produits Big-IP.

Big-IP est un contrôleur de livraison d'applications *ADC (Application Delivery Controller),* son objectif est d'améliorer les performances via une optimisation des flux de données au travers des réseaux *ADN (Application Delivery Network).*

IControl REST est la nouvelle version d'*IControl*, il s'agit d'une API qui permet de faciliter l'interaction entre l'utilisateur et les équipements de l'entreprise F5.

La vulnérabilité a été identifiée dans /mgmt/tm/util/bash de l'API *iControl REST* lors d'une étude interne réalisée par l'entreprise F5. Il est possible d'envoyer des requêtes http POST malveillantes vers le port de gestion ou sa propre adresse IP, afin de contourner la politique de sécurité et de porter atteinte à l'intégrité des données qui sont stockées sur le système Big-IP. L'exploitation de cette vulnérabilité par un attaquant distant et non authentifié peut permettre l'exécution de code arbitraire et la compromission totale du système ciblé.

Cette vulnérabilité est activement exploitée et un POC est disponible en sources ouvertes.

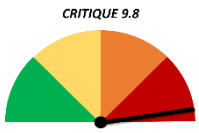
Dans un article publié par Unit42 le 10 mai 2022, l'entreprise Palo Alto Networks révèle avoir défini la signature Threat Prevention 92570 pour la CVE-2022-1388 et qu'en seulement 10 heures, la signature aurait été déclenchée 2552 fois à la suite de plusieurs tentatives d'exploitations.

L'entreprise F5 recommande d'appliquer les mises à jour au plus vite.

01.2 INFORMATIONS

01.2.1 | RISQUES

- Exécution de code arbitraire à distance
- Atteinte à l'intégrité des données
- Contournement de la politique de sécurité



01.2.2 | CRITICITE

- **La faille est activement exploitée**
- **Vecteur d'attaque : Réseau**
- **Complexité d'attaque : Faible**
- **Privilèges requis : Aucun**

- **Interaction de l'utilisateur : Non**
- **Portée : Inchangée**
- **Impact sur la confidentialité : Haute**
- **Impact sur l'intégrité : Haute**
- **Impact sur la disponibilité : Haute**

01.2.3 | CVE

- CVE-2022-1388

01.2.4 | COMPOSANTS VULNERABLES.

Ci-dessous, la liste des produits concernés :

- BIG-IP (tous les modules), version 16.1.0 à 16.1.2
- BIG-IP (tous les modules), version 15.1.0 à 15.1.5
- BIG-IP (tous les modules), version 14.1.0 à 14.1.4
- BIG-IP (tous les modules), version 13.1.0 à 13.1.4
- BIG-IP (tous les modules), version 12.1.0 à 12.1.6
- BIG-IP (tous les modules), version 11.6.1 à 11.6.5

01.3 RECOMMANDATIONS

- Pour BIG-IP (tous les modules), version 16.1.0 à 16.1.2, appliquer la mise à jour vers la version 16.1.2.2.
- Pour BIG-IP (tous les modules), version 15.1.0 à 15.1.5, appliquer la mise à jour vers la version 15.1.5.1.
- Pour BIG-IP (tous les modules), version 14.1.0 à 14.1.4, appliquer la mise à jour vers la version 14.1.4.6.
- Pour BIG-IP (tous les modules), version 13.1.0 à 13.1.4, appliquer la mise à jour vers la version 13.1.5.
- Pour BIG-IP (tous les modules), version 12.1.0 à 12.1.6, aucune mise à jour ne sera réalisée par l'éditeur.
- Pour BIG-IP (tous les modules), version 11.6.1 à 11.6.5, aucune mise à jour ne sera réalisée par l'éditeur.
- Des informations complémentaires ainsi qu'une solution d'atténuation sont disponibles ici : K23605346

- Les produits suivants ne sont pas impactés par la vulnérabilité : BIG-IQ Centralized Management, F5OS-A, F5OS-C et Traffix SDC.
- L'entreprise F5 a publié le 28 novembre 2018 une documentation d'aide pour l'utilisateur en cas de suspicion de compromission d'un système Big-IP. La documentation est disponible ici : K11438344

01.4 PROOF OF CONCEPT

Un exploit (POC) est disponible en sources ouvertes.

02 REFERENCES

https://nvd.nist.gov/vuln/detail/CVE-2022-1388

https://support.f5.com/csp/article/K23605346

https://support.f5.com/csp/article/K23605346

https://support.f5.com/csp/article/K84205182

https://www.cybersecurity-help.cz/vdb/SB2022051005

https://clouddocs.f5.com/api/icontrol-rest/

https://sensorstechforum.com/fr/cve-2022-1388-exploited/

https://unit42.paloaltonetworks.com/cve-2022-1388/

advens.fr

Lille +33 3 20 68 41 81
Paris +33 1 84 16 30 25
Lyon +33 4 28 29 08 29
Bordeaux +33 5 35 54 82 84