Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 12 août 2016
N° CERTFR-2016-AVI-280

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits F5 BIG-IP

Gestion du document

Référence	CERTFR-2016-AVI-280
Titre	Multiples vulnérabilités dans les produits F5 BIG-IP
Date de la première version	12 août 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité F5 SOL12401251 du 10 août 2016 Bulletin de sécurité F5 SOL31925518 du 10 août 2016 Bulletin de sécurité F5 SOL10133477 du 10 août 2016
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

- exécution de code arbitraire à distance
- déni de service à distance
- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- F5 BIG-IP LTM, BIG-IP AAM, BIG-IP AFM, BIG-IP Analytics, BIG-IP APM, BIG-IP ASM, BIG-IP Link Controller et BIG-IP PEM en versions 11.4.0 à 11.5.4 HF1, 11.6.0 et 12.0.0 à 12.0.0 HF1
- F5 BIG-IP LTM, BIG-IP Analytics, BIG-IP APM, BIG-IP ASM, BIG-IP Link Controller et BIG-IP GTM en versions 11.2.1 à 11.2.1 HF15
- F5 BIG-IP GTM en versions 11.4.0 à 11.5.4 HF1 et 11.6.0
- F5 BIG-IP PSM en versions 11.4.0 à 11.4.1
- F5 BIG-IP Edge Gateway, BIG-IP WebAccelerator et BIG-IP WOM en versions 11.0.0 à 11.3.0
- F5 BIG-IP LTM, BIG-IP AAM, BIG-IP AFM, BIG-IP APM, BIG-IP ASM, BIG-IP Link Controller, BIG-IP PEM et BIG-IP GTM en versions 11.0.0 à 11.6.0
- F5 BIG-IP Analytics en versions 12.0.0 et 11.0.0 à 11.6.0
- F5 BIG-IP DNS en versions 12.0.0 à 12.0.0 HF1

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits F5 BIG-IP*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité F5 SOL12401251 du 10 août 2016
  https://support.f5.com/kb/en-us/solutions/public/k/12/sol12401251.html
- Bulletin de sécurité F5 SOL31925518 du 10 août 2016
  https://support.f5.com/kb/en-us/solutions/public/k/31/sol31925518.html
- Bulletin de sécurité F5 SOL10133477 du 10 août 2016
  https://support.f5.com/kb/en-us/solutions/public/k/10/sol10133477.html
- Référence CVE CVE-2016-5736
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5736
- Référence CVE CVE-2016-1497
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1497
- Référence CVE CVE-2015-8022
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8022

Gestion détaillée du document

12 août 2016 version initiale.