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 22 avril 2014
N° CERTFR-2014-AVI-200

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits F5

Gestion du document

Référence	CERTFR-2014-AVI-200
Titre	Multiples vulnérabilités dans F5
Date de la première version	22 avril 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité F5 sol15172 du 17 avril 2014 Bulletin de sécurité F5 sol15158 du 17 avril 2014 Bulletin de sécurité F5 sol15180 du 17 avril 2014 Bulletin de sécurité F5 sol15189 du 18 avril 2014
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)

- déni de service à distance

2 - Systèmes affectés

- F5 BIG-IP LTM versions 10.0.0 à 10.2.4
- F5 BIG-IP LTM versions 11.0.0 à 11.5.1
- F5 BIG-IP AAM versions 11.4.0 à 11.5.1
- F5 BIG-IP AFM versions 11.3.0 à 11.5.1
- F5 BIG-IP Analytics versions 11.0.0 à 11.5.1
- F5 BIG-IP APM versions 10.1.0 à 10.2.4
- F5 BIG-IP APM versions 11.0.0 à 11.5.1
- F5 ARX versions 6.0.0 à 6.4.0
- F5 BIG-IP ASM versions 10.0.0 à 10.2.4
- F5 BIG-IP ASM versions 11.0.0 à 11.5.1
- F5 BIG-IP Edge Gateway versions 10.1.0 à 10.2.4
- F5 BIG-IP Edge Gateway versions 11.0.0 à 11.3.0
- F5 BIG-IP GTM versions 10.0.0 à 10.2.4

- F5 BIG-IP GTM versions 11.0.0 à 11.5.1
- F5 BIG-IP Link Controller versions 10.0.0 à 10.2.4
- F5 BIG-IP Link Controller versions 11.0.0 à 11.5.1
- F5 BIG-IP PEM versions 11.3.0 à 11.5.1
- F5 BIG-IP PSM versions 10.0.0 à 10.2.4
- F5 BIG-IP PSM versions 11.0.0 à 11.4.1
- F5 BIG-IP WebAccelerator versions 10.0.0 à 10.2.4
- F5 BIG-IP WebAccelerator versions 11.0.0 à 11.3.1
- F5 BIG-IP WOM versions 10.0.0 à 10.2.4
- F5 BIG-IP WOM versions 11.0.0 à 11.3.0
- F5 Enterprise Manager versions 2.1.0 à 2.3.0
- F5 Enterprise Manager versions 3.0.0 à 3.1.1

3 - Résumé

De multiples vulnérabilités ont été corrigées dans les produits *F5*. Elles permettent à un attaquant de provoquer un déni de service à distance.

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 sol15172 du 17 avril 2014
  http://support.f5.com/kb/en-us/solutions/public/15000/100/sol15172.html
- Bulletin de sécurité F5 sol15158 du 17 avril 2014
  http://support.f5.com/kb/en-us/solutions/public/15000/100/sol15158.html
- Bulletin de sécurité F5 sol15180 du 17 avril 2014
  http://support.f5.com/kb/en-us/solutions/public/15000/100/sol15180.html
- Bulletin de sécurité F5 sol15189 du 18 avril 2014
  http://support.f5.com/kb/en-us/solutions/public/15000/100/sol15189.html
- Référence CVE CVE-2010-3762
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3762
- Référence CVE CVE-2013-6450
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6450
- Référence CVE CVE-2013-4353
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4353
- Référence CVE CVE-2014-0050
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0050

Gestion détaillée du document

22 avril 2014 version initiale.