

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans F5 FirePass

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-322>

---

### Gestion du document

Référence	CERTA-2010-AVI-322
Titre	Vulnérabilités dans F5 FirePass
Date de la première version	19 juillet 2010
Date de la dernière version	–
Source(s)	Bulletins de sécurité F5 SOL11795 et SOL11797 du 07 juillet 2010
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

- Contournement de la politique de sécurité ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

- FirePass version 5.x ;
- FirePass version 6.x.

## 3 Résumé

Deux vulnérabilités dans F5 FirePass permettent de contourner la politique de sécurité ou d'effectuer une injection de code indirecte.

## 4 Description

Deux vulnérabilités ont été découvertes dans F5 FirePass :

- une vulnérabilité de type injection de code indirecte est présente dans la page de pré-authentification ;

- une erreur dans la gestion de la séquence d'authentification permet à une personne malintentionnée de contourner la phase de vérification de conformité de la machine avant l'accès à la page d'authentification.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité F5 SOL11795 du 07 juillet 2010 :  
<http://support.f5.com/kb/en-us/solutions/public/11000/700/sol11795.html>
- Bulletin de sécurité F5 SOL11797 du 07 juillet 2010 :  
<http://support.f5.com/kb/en-us/solutions/public/11000/700/sol11797.html>

## **Gestion détaillée du document**

**19 juillet 2010** version initiale.