

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans les produits Cisco PIX, ASA et FWSM

---

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-2006-AVI-186>

---

### Gestion du document

Référence	CERTA-2006-AVI-186
Titre	Vulnérabilité dans les produits Cisco PIX, ASA et FWSM
Date de la première version	10 mai 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #70090 du 8 mai 2006
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.

## 2 Systèmes affectés

- Cisco PIX 6.x ;
- Cisco PIX 7.x ;
- Cisco Adaptive Security Appliance (ASA) 7.x ;
- Cisco Firewall Services Module (FWSM) 2.x ;
- Cisco Firewall Services Module (FWSM) 3.x.

## 3 Résumé

Une vulnérabilité dans les produits Cisco PIX, ASA et FWSM permet à un utilisateur distant de contourner la politique de sécurité du système.

## **4 Description**

Une erreur dans le traitement des requêtes HTTP fragmentées sur les produits Cisco PIX, ASA et FWSM permet de contourner les règles de filtrage de liens créées par l'intermédiaire du logiciel Websense. Ceci rend possible, pour un utilisateur distant mal intentionné, l'accès à certaines parties normalement inaccessibles d'un site web protégé par l'équipement vulnérable.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Cisco ID du 10 mai 2006 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20060508-pix.shtml>
- Référence CVE CVE-2006-0515 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0515>

## **Gestion détaillée du document**

**10 mai 2006** version initiale.