



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 23 octobre 2008  
N° CERTA-2008-AVI-522

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Cisco PIX et ASA

---

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-2008-AVI-522>

---

### Gestion du document

Référence	CERTA-2008-AVI-522
Titre	Vulnérabilités dans Cisco PIX et ASA
Date de la première version	23 octobre 2008
Date de la dernière version	–
Source(s)	Avis de sécurité 108009 de Cisco publié le 22 octobre 2008
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

- Déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Cisco ASA 5500 ;
- Cisco PIX.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les produits de sécurité Cisco ASA et Cisco PIX. L'exploitation de ces dernières permet de perturber le fonctionnement du système vulnérable ou de contourner la politique de sécurité mise en place.

## 4 Description

Plusieurs vulnérabilités ont été identifiées dans les produits de sécurité Cisco ASA et Cisco PIX :

- certains systèmes Cisco ASA ou PIX configurés avec IPSec ou un accès distant VPN basé sur SSL peuvent être trompés par une personne malveillante qui contournerait la phase d'authentification par domaine Windows NT. Les autres méthodes d'authentification externes (LDAP, RADIUS, TACACS+, etc.) ne sont pas concernées ;
- certains systèmes Cisco ASA ou PIX utilisant des logiciels de version 7.2(4)9 ou 7.2(4)10 n'interprètent pas correctement des trames IPv6. L'exploitation de cette vulnérabilité peut provoquer le dysfonctionnement du système ;
- certains systèmes Cisco ASA (versions 8.0.x) n'interprètent pas correctement des trames qui nécessitent l'usage de l'accélérateur de chiffrement. Plusieurs services y ont recours.

## 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 20081022-asa du 22 octobre 2008 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20081022-asa.shtml>
- Référence CVE CVE-2008-3815 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3815>
- Référence CVE CVE-2008-3816 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3816>
- Référence CVE CVE-2008-3817 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3817>

## Gestion détaillée du document

23 octobre 2008 version initiale.