

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités du garde-barrière PIX de Cisco

---

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-2003-AVI-208>

---

### Gestion du document

Référence	CERTA-2003-AVI-208
Titre	Multiples vulnérabilités du garde-barrière PIX de Cisco
Date de la première version	16 décembre 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Cisco
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.

## 2 Systèmes affectés

La première vulnérabilité affecte les versions suivantes :

- 6.3.1 ;
- 6.2.2 et antérieures ;
- 6.1.4 et antérieures ;
- 5.X.X et antérieures.

La seconde vulnérabilité affecte les versions 6.2.3 et antérieures. Les versions 6.1.X et 5.X.X ne disposant pas du client VPN ne sont pas affectées.

## 3 Résumé

Deux nouvelles vulnérabilités ont été découvertes dans le garde-barrière PIX de Cisco.

## 4 Description

- Première vulnérabilité : au moyen d'un message SNMPv3 habilement constitué, un utilisateur mal intentionné peut forcer l'arrêt brutal du garde-barrière. Cette vulnérabilité n'est exploitable que si le garde-barrière est configuré pour recevoir les messages SNMP (`snmp-server host <adresseIP>`).
- Deuxième vulnérabilité : il est possible, sous certaines circonstances, de forcer le client VPN du garde-barrière Cisco à supprimer un tunnel IPSEC préalablement établi.

## 5 Contournement provisoire

Deux mesures de protection peuvent être mises en oeuvre pour prévenir l'exploitation de la première vulnérabilité :

- Restreindre l'accès au serveur SNMP du garde-barrière :  
`snmp-server host <interface> <adresseIp> poll`
- ou arrêter le serveur SNMP du garde-barrière :  
`no snmp-server location`  
`no snmp-server contact`  
`snmp-server community public`  
`no snmp-server enable-traps`

## 6 Solution

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

## 7 Documentation

Bulletin de sécurité de Cisco :  
<http://www.cisco.com/warp/public/707/cisco-sa-20031215-pix.shtml>

## Gestion détaillée du document

16 décembre 2003 version initiale.