Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 novembre 2002
N° CERTA-2002-AVI-250

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le garde-barrière PIX de CISCO

Gestion du document

Référence	CERTA-2002-AVI-250
Titre	Multiples vulnérabilités dans le garde-barrière PIX de CISCO
Date de la première version	21 novembre 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

- Vol d'une session VPN ;
- déni de service.

2 Systèmes affectés

La première vulnérabilité affecte les versions suivantes :
- 6.0.3 et précédentes ;
- 6.1.3 et précédentes.

La seconde vulnérabilité affecte les versions :
- 5.2.8 et précédentes ;
- 6.0.3 et précédentes ;
- 6.1.3 et précédentes ;
- 6.2.1 et précédentes.

3 Résumé

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

4 Description

- Lors de l'établissement d'une session VPN (Virtual Private Network) avec un utilisateur, le garde-barrière crée un contexte de sécurité (ISAKMP SA) associant l'utilisateur et son adresse IP.
  Une vulnérabilité dans la gestion de ce contexte permet à un utilisateur mal intentionné de voler une session établie entre un utilisateur authentifié et le garde-barrière.
- Un dédordement de mémoire peut être effectué lors de requêtes HTTP pour une authentification utilisant un système RADIUS ou TACACS+ afin de stopper et redémarrer le PIX.

5 Solution

Appliquer la mise à jour de la version du garde-barrière selon la version affectée (cf. Documentration).

6 Documentation

Bulletin de sécurité "Cisco PIX Multiple Vulnerabilities" de CISCO :
http://www.cisco.com/warp/public/707/pix-multiple-vuln-pub.shtml

Gestion détaillée du document

21 novembre 2002 version initiale.