Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 octobre 2001
N° CERTA-2001-AVI-108

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le garde-barrière PIX de Cisco

Gestion du document

Référence	CERTA-2001-AVI-108
Titre	Vulnérabilité dans le garde-barrière PIX de Cisco
Date de la première version	04 octobre 2001
Date de la dernière version	–
Source(s)	Avis de sécurité Cisco "Cisco PIX firewall authetication denial of service vulnerability"
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

Les versions du garde-barrière PIX 4.0 à 4.4(8), 5.0(3), 5.1(3), 5.2(2) et 5.3(1) sont affectées.
Seuls les systèmes utilisant le service d'authentification AAA sont concernés.

3 Résumé

En exploitant une vulnérabilité dans le module d'authentification, un utilisateur mal intentionné peut provoquer un déni de service sur le garde-barrière PIX de Cisco.

4 Description

Un utilisateur mal intentionné peut réaliser un déni de service en envoyant de nombreuses requêtes d'authentification et provoquer ainsi un épuisement des ressources du garde-barrière.

Selon Cisco, ce déni de service empêche les utilisateurs légitimes de pouvoir s'authentifier et peut porter atteinte à la disponibilité du garde-barrière.

Cette vulnérabilité n'est exploitable que si le service d'authentification AAA est activé (existence de lignes de configuration commençant par `aaa authentication`).

5 Solution

Les version 5.2(6) et 5.3(2) corrigent le problème.

6 Documentation

Avis de sécurité Cisco "Cisco PIX firewall authetication denial of service vulnerability" :
http://www.cisco.com/warp/public/707/pixfirewall-authen-flood-pub.shtml

Gestion détaillée du document

04 octobre 2001 version initiale.