Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 septembre 2001
N° CERTA-2001-AVI-102

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le garde-barrière PIX de Cisco

Gestion du document

Référence	CERTA-2001-AVI-102
Titre	Vulnérabilité dans le garde-barrière PIX de Cisco
Date de la première version	28 septembre 2001
Date de la dernière version	–
Source(s)	Bulletin 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

Contournement des règles de filtrage.

2 Systèmes affectés

Les gardes-barrières Cisco Secure PIX versions 4.4, 5.1, 5.2, 5.3 et 6.0.

3 Résumé

Un utilisateur mal intentionné peut contourner les règles de filtrage des commandes SMTP (Simple Mail Tranfert Protocol).

4 Description

Une fonctionnalité "mailguard" du garde-barrière Cisco PIX permet de limiter les commandes SMTP à un jeu très restreint de commandes. Une vulnérabilité dans le filtrage permet à un utilisateur mal intentionné de contourner ces règles de filtrage et d'attaquer alors le serveur de courrier se trouvant derrière le garde-barrière. Si

la configuration du serveur est trop permissive, l'attaquant pourra alors récupérer des informations sur les comptes du serveur, ou exécuter du code arbitraire à distance.

5 Solution

Appliquer les correctifs Cisco suivants les versions de Cisco PIX. Ces correctifs se trouvent sur le site de Cisco.

http://www.cisco.com

6 Documentation

Bulletin de sécurité Cisco :
http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-regression-pub.shtml

Gestion détaillée du document

28 septembre 2001 version initiale.