Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 septembre 2000
N° CERTA-2000-AVI-054

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le garde barrière PIX de CISCO

Gestion du document

Référence	CERTA-2000-AVI-054
Titre	Vulnérabilité dans le garde barrière PIX de CISCO
Date de la première version	29 septembre 2000
Date de la dernière version	–
Source(s)	Bulletin Cisco Bugtraq
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

- Toutes versions de CISCO PIX jusqu'à 4.4(5) ;
- Versions CISCO PIX 5.0.x jusqu'à 5.0(3) ;
- Versions CISCO PIX 5.1.x jusqu'à 5.1(2) ;
- Version CISCO PIX 5.2(1).

3 Résumé

Un utilisateur distant mal intentionné peut contourner les règles de filtrage d'un garde barrière CISCO PIX afin de recueillir des informations par le biais de commandes SMTP.

4 Description

Une fonctionnalité « mailguard » du garde barrière CISCO PIX permet de limiter l'utilisation des commandes SMTP « Simple Mail Transfert Protocol ». Cette limitation a pour but d'empêcher les utilisateurs distants de recueillir, en utilisant des commandes SMTP, des informations comme par exemple, les utilisateurs du système.

Une vulnérabilité de « mailguard » permet à un utilisateur distant mal intentionné de contourner ces limitations afin de pouvoir utiliser toutes les commandes SMTP. Un programme permettant d'exécuter ce contournement a été diffusé sur Internet.

5 Solution

Correctifs à appliquer suivant les versions de PIX :

- Toutes versions de CISCO PIX jusqu'à 4.4(5) : Correctif 4.4(6) ;
- Versions CISCO PIX 5.0.x jusqu'à 5.0(3) : Correctif 5.1(3) ;
- Versions CISCO PIX 5.1.x jusqu'à 5.1(2) : Correctif 5.1(3) ;
- Version CISCO PIX 5.2(1) : Correctif 5.2(2).

Ces correctifs sont disponibles sur le site CISCO :
http://www.cisco.com

6 Documentation

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

Gestion détaillée du document

29 septembre 2000 version initiale.