Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 août 2006
N° CERTA-2006-AVI-371

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits pare-feux de Cisco

Gestion du document

Référence	CERTA-2006-AVI-371
Titre	Vulnérabilité dans les produits pare-feux de Cisco
Date de la première version	24 août 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco ID-70811 du 23 août 2006
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 à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Cisco PIX 500 Series Security Appliances, ayant une version logicielle de la forme 7.0(x) antérieure ou égale à 7.0(5) ;
- Cisco PIX 500 Series Security Appliances, ayant une version logicielle 7.1(x) antérieure ou égale à 7.1(2.4) ;
- Cisco ASA 5500 Series Adaptive Security Appliances, ayant une version logicielle de la forme 7.0(x) antérieure ou égale à 7.0(5) ;
- Cisco ASA 5500 Series Adaptive Security Appliances, ayant une version logicielle 7.1(x) antérieure ou égale à 7.1(2.4) ;
- le module FWSM (pour *Firewall Services Module*) des Cisco Catalyst 6500 Switches et Cisco 7600 Series Routers, ayant une version de la forme 3.1(x) antérieure ou égale à 3.1(1.6).

3 Résumé

Une vulnérabilité a été identifiée dans certaines versions du logiciel commun à plusieurs produits de sécurité Cisco. Une personne malveillante pourrait, à distance, exploiter celle-ci, afin de modifier les mots de passe des utilisateurs du système Cisco, ou activer des mots de passe afin d'en bloquer l'accès aux administrateurs légitimes.

4 Description

Les produits de sécurité Cisco mettent en œuvre plusieurs procédés d'authentification, notamment pour les différents modes de configuration (`EXEC mode` ou `enable mode` par exemple). Les méthodes dites `AAA` (pour *Authentification, Authorization,and Accounting*) sont régulièrement déployées, sous la forme de `RADIUS`, `TACACS+` ou `LOCAL`. Quand ce n'est pas le cas, l'authentification se fait par le biais de commandes spécifiques :

- la commande `passwd` pour le mode `EXEC` ;
- la commande `enable password` pour le mode `enable` ;
- la commande `username` pour configurer les utilisateurs locaux ainsi que leurs mots de passe.

Une vulnérabilité a été identifiée dans l'étape de vérification de la configuration, et pourrait conduire au changement de mot de passe sans aucune intervention d'un utilisateur légitime. Une personne malveillante, peut, sous certaines conditions, tirer profit de cette vulnérabilité pour empêcher l'accès au système vulnérable.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco ID 70811 cisco-sa-20060823-firewall du 23 août 2006 :
  http://www.cisco.com/warp/public/707/cisco-sa-20060823-firewall.shtml

Gestion détaillée du document

24 août 2006 version initiale.