Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 décembre 2003
N° CERTA-2003-AVI-209

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du module Cisco Firewall Services (FWSM)

Gestion du document

Référence	CERTA-2003-AVI-209
Titre	Multiples vulnérabilités du module Cisco Firewall Services (FWSM)
Date de la première version	16 décembre 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité de 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

Déni de service.

2 Systèmes affectés

Cisco FWSM versions 1.1.2 et antérieures.

3 Résumé

Deux vulnérabilités ont été découvertes dans le module Cisco Firewall Services (FWSM) pour les équipements Cisco Catalyst 6500 et 7600.

4 Description

– Première vulnérabilité : au moyen d'un message SNMPv3 habilement constitué, un utilisateur mal intentionné peut forcer l'arrêt brutal du module FWSM. Cette vulnérabilité n'est exploitable que si le module FWSM est configuré pour recevoir les messages SNMP (`snmp-server host <adresseIP>`).

– Deuxième vulnérabilité : une vulnérabilité de type débordement de mémoire est présente lors du traitement de l'authentification auprès d'un serveur TACACS+ ou RADIUS d'un utilisateur se connectant via les protocoles FTP, TELNET ou HTTP.

5 Contournement provisoire

Deux mesures de protection peuvent être mises en oeuvre pour prévenir l'exploitation de la première vulnérabilité :

– Restreindre l'accès au serveur SNMP du garde-barrière :

```
snmp-server host <interface> <adresseIp> poll
```

– ou arrêter le serveur SNMP du garde-barrière :

```
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable-traps
```

6 Solution

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

7 Documentation

Bulletin de sécurité de Cisco :
http://www.cisco.com/warp/public/707/cisco-sa-20031215-fwsm.shtml

Gestion détaillée du document

16 décembre 2003 version initiale.