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 février 2011
N° CERTA-2011-AVI-104

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco Firewall Services Module

Gestion du document

Référence	CERTA-2011-AVI-104
Titre	Vulnérabilité dans Cisco Firewall Services Module
Date de la première version	24 février 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco-sa-20110223-fwsm
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 Firewall Services Module 3.x ;
- Cisco Firewall Services Module 4.x.

3 Résumé

Une vulnérabilité permettant d'effectuer un déni de service à distance a été identifiée dans le produit Cisco Firewall Services Module (FWSM).

4 Description

Une vulnérabilité dans le module d'inspection de trafic `SCCP` (protocole `Skinny`) peut entrainer un rechargement de la configuration de l'équipement lors du traitement d'un paquet spécifiquement conçu. Par défaut, l'inspection du trafic `SCCP` est activée.

5 Solution

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

Les versions 3.1(20), 3.2(20), 4.0(15) et 4.1(5) corrigent ce problème. Il est aussi possible de déscativer l'inspection du trafic `SCCP` via la commande `no inspect skinny` si ce protocole n'est pas utilisé dans le réseau.

6 Documentation

- Bulletin de sécurité Cisco 20110223-fwsm du 23 février 2011 :
  http://www.cisco.com/warp/public/707/cisco-sa-20110223-fwsm.shtml
- Référence CVE CVE-2011-0394 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0394

Gestion détaillée du document

24 février 2011 version initiale.