



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 mai 2008
N° CERTA-2008-AVI-253

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits Cisco CSM

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-253>

Gestion du document

Référence	CERTA-2008-AVI-253
Titre	Vulnérabilité dans les produits Cisco CSM
Date de la première version	19 mai 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco n105450 du 14 mai 2008
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.

2 Systèmes affectés

- Cisco Catalyst Content Switching Module (CSM) 4.x ;
- Cisco Catalyst Content Switching Module with SSL (CSM-S) 2.x.

3 Résumé

Une vulnérabilité dans les produits Cisco de type CSM et CSM-S permet à un utilisateur distant de provoquer un déni de service à distance.

4 Description

Une vulnérabilité de type « fuite mémoire » est présente dans les extensions Cisco Catalyst Content Switching Module (CSM) 4.x et leur version supportant le SSL : CSM-S. Cette vulnérabilité permet à un

utilisateur distant de provoquer une consommation excessive de la mémoire par l'équipement vulnérable via des paquets TCP particuliers.

L'exploitation de cette vulnérabilité nécessite que les équipements CSM ou CSM-S soient configurés en mode *layer 7 load balancing*.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco ID 105450 du 14 mai 2008 :
<http://www.cisco.com/warp/public/707/cisco-sa-20080514-csm.shtml>
- Référence CVE CVE-2008-1749 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1749>

Gestion détaillée du document

19 mai 2008 version initiale.