



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 11 septembre 2007  
N° CERTA-2007-AVI-396

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités des produits Cisco Catalyst

---

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-2007-AVI-396>

---

### Gestion du document

Référence	CERTA-2007-AVI-396
Titre	Vulnérabilités des produits Cisco Catalyst
Date de la première version	11 septembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 97826 du 5 septembre 2007
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

- CSM Version 4.2;
- CSM-S Version 2.1.

## 3 Résumé

Les produits CSM (Content Switching Modules) et CSM-S (Content Switching Modules SSL) sont affectés par deux vulnérabilités permettant un déni de service à distance.

## 4 Description

Les modules Cisco CSM (Content Switching Modules) et CSM-S (Content Switching Modules SSL) sont des répartiteurs de charge permettant d'optimiser les temps de réponse des réseaux. Ils sont affectés par deux vulnérabilités touchant le traitement des paquets de type TCP, et les équipements avec l'option *service termination* activée.

## **5 Solution**

Se référer au bulletin de sécurité Cisco 97826 du 5 septembre 2007 pour l'obtention des correctifs (cf. section Documentation).

## **6 Documentation**

- Bulletin de sécurité Cisco ID 97826 du 5 septembre 2007 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20070905-csm.shtml>

## **Gestion détaillée du document**

**11 septembre 2007** version initiale.