

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans les commutateurs CISCO Catalyst 4000, 5000 et 6000

---

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-2000-AVI-086>

---

### Gestion du document

Référence	CERTA-2000-AVI-086
Titre	Vulnérabilité dans les commutateurs CISCO Catalyst 4000, 5000 et 6000
Date de la première version	08 décembre 2000
Date de la dernière version	–
Source(s)	Avis 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

- Catalyst 4000 et 5000 - version logicielle 4.5(2) à 5.5(4) et 5.5(4.a) ;
- Catalyst 6000 - version logicielle 5.3(1)CSX à 5.5(4) et 5.5(4.a).

## 3 Description

Un utilisateur mal intentionné, effectuant une série rapide de fausses authentifications telnet, peut provoquer un déni de service obligeant le redémarrage du commutateur.

Nota : Tous les types d'authentification telnet ( Kerberos ) sont concernés par cette vulnérabilité.

## 4 Contournement provisoire

Installer une liste de contrôle d'accès sur le commutateur :  
set ip permit enable telnet

set ip permit <addr> [mask]

Désactiver la gestion de commande à distance.

## **5 Solution**

Appliquer le correctif fourni par CISCO :  
<http://www.cisco.com>

## **6 Documentation**

Avis de sécurité CISCO :  
<http://www.cisco.com/warp/public/707/catalyst-memleak-pub.shtml>

## **Gestion détaillée du document**

**08 décembre 2000** version initiale.