

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité des Cisco IOS et CatOS sous le protocole CDP

---

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-2001-AVI-121>

---

### Gestion du document

Référence	CERTA-2001-AVI-121
Titre	Vulnérabilité des Cisco IOS et CatOS sous le protocole CDP
Date de la première version	19 octobre 2001
Date de la dernière version	–
Source(s)	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 CatOS;
- Cisco IOS.

## 3 Résumé

Un utilisateur mal intentionné, se trouvant sur un réseau comportant des équipements CISCO, peut réaliser un déni de service de ces derniers via le protocole CDP.

## 4 Description

CDP (Cisco Discovery Protocol) est un protocole permettant aux équipements CISCO d'un même réseau de s'échanger des informations. Ce protocole permet, par l'envoi de trames périodiques, de tenir à jour une table d'information d'états des matériels CISCO voisins (adresses, etc.)

Un utilisateur mal intentionné peut réaliser un déni de service sur les équipements CISCO par l'envoi massif de requêtes CDP. Cette vulnérabilité n'est exploitable que par une machine se trouvant sur le même réseau physique que le CISCO (CDP utilisant des trames de diffusion de niveau 2 non routables).

Le protocole CDP est activé par défaut sur les CISCO.

## **5 Contournement provisoire**

Désactiver le protocole CDP sur le matériel vulnérable (cf section documentation).

## **6 Solution**

Les correctifs pour Cisco IOS sont disponibles sur le site CISCO:

<http://www.cisco.com>

Les correctifs pour Cisco CatOS ne sont pas disponibles actuellement sur le site CISCO.

## **7 Documentation**

Note d'information CISCO :

[http://www.cisco.com/warp/public/707/cdp\\_issue.shtml](http://www.cisco.com/warp/public/707/cdp_issue.shtml)

## **Gestion détaillée du document**

**19 octobre 2001** version initiale.