

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans CISCO CatOS

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-2003-AVI-103>

Gestion du document

Référence	CERTA-2003-AVI-103
Titre	Vulnérabilité dans CISCO CatOS
Date de la première version	10 juillet 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO : "Denial-of-Service of TCP-based Services in CatOS"
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

CatOs pour tous les commutateurs Catalyst suivants :

- Catalyst série 4000 incluant les modèles 2948G et 2980G/2980G-A ;
- Catalyst série 5000 incluant les modèles 2901, 2902 et 2926 ;
- Catalyst 6000.

3 Résumé

Une vulnérabilité présente dans CatOS permet à un utilisateur mal intentionné d'effectuer un déni de service sur les commutateurs CISCO.

4 Description

L'envoi de paquets TCP avec certaines combinaisons de drapeaux non standard vers le service d'un commutateur permet d'effectuer un déni de service sur les équipements vulnérables.

5 Solution

Se référer au bulletin de sécurité Cisco (cf. section Documentation) pour l'obtention d'un correctif.

6 Documentation

Bulletin de sécurité CISCO "Denial-of-Service of TCP-based Services in CatOS":
<http://www.cisco.com/warp/public/707/cisco-sa-20030709-swtcp.shtml>

Gestion détaillée du document

10 juillet 2003 version initiale.