Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 juin 2004
N° CERTA-2004-AVI-191

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Cisco CatOS

Gestion du document

Référence	CERTA-2004-AVI-191
Titre	Vulnérabilité de Cisco CatOS
Date de la première version	10 juin 2004
Date de la dernière version	–
Source(s)	Avis de sécurité "Cisco CatOS Telnet, HTTP and SSH vulnerability" de 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

Les commutateurs Catalyst suivants :

- Catalyst série 6000 ;
- Catalyst série 5000 ;
- Catalyst série 4500 ;
- Catalyst série 4000 ;
- Catalyst 2948G, 2980G, 2980G-A, 4912G
- Catalyst 2901, 2902, 2926(T,F,GS,GL), 2948.

avec les versions de CatOS égales ou antérieures à :

- 8.3(2)GLX ;
- 8.2(2) ;
- 7.6(6) ;
- 6.4(9) ;
- 5.5(20).

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

Sur un système vulnérable, si la phase d'établissement de connexion TCP n'est pas terminée, il est possible de réaliser un déni de service sur le système cible par consommation excessive des ressources.

Selon Cisco, l'exploitation de cette vulnérabilité n'est possible que sur un système ayant les services Telnet, HTTP ou SSH activés.

5 Contournement provisoire

Désactiver les services ou mettre en place des filtres afin de restreindre l'accès au services Telnet, HTTP ou SSH.

6 Solution

Se référer au bulletin de sécurité du constructeur pour l'obtention des correctifs.

7 Documentation

Avis de sécurité "Cisco CatOS Telnet, HTTP and SSH vulnerability" de Cisco :
http://www.cisco.com/warp/public/707/cisco-sa-20040609-catos.shtml

Gestion détaillée du document

10 juin 2004 version initiale.