Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 avril 2003
N° CERTA-2003-AVI-079

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des commutateurs Catalyst de Cisco

Gestion du document

Référence	CERTA-2003-AVI-079
Titre	Vulnérabilité des commutateurs Catalyst de Cisco
Date de la première version	25 avril 2003
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

- Accès non autorisé ;
- élévation de privilèges.

2 Systèmes affectés

Les commutateurs Cisco Catalyst 4000, 6000 et 6500 utilisant Catalyst OS version 7.5(1).

3 Description

Selon Cisco, un utilisateur non autorisé peut obtenir un accès à un système vulnérable en local (via la console) ou à distance (accès `ssh` ou `telnet`) sans connaissance d'un mot de passe valide.

Il est également possible de passer en mode privilégié (`"enable"`) et modifier ainsi la configuration du commutateur.

La vulnérabilité ne peut être exploitée que sur des configurations utilisant une authentification locale.

4 Contournement provisoire

Il est possible de spécifier les machines pouvant accéder aux services `ssh` et `telnet` du commutateur au moyen d'une liste de controle d'accès :

```
set ip permit <adresse> <masque> telnet
set ip permit <adresse> <masque> ssh
set ip permit enable
```

5 Solution

La version 7.6(1) de Cisco Catalyst OS corrige cette vulnérabilité.

6 Documentation

Avis de sécurité de Cisco "Cisco Catalyst enable password bypass vulnerability" :
http://www.cisco.com/warp/public/707/cisco-sa-20030424-catos.shtml

Gestion détaillée du document

25 avril 2003 version initiale.