Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 janvier 2002
N° CERTA-2002-AVI-017

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de `telnet` sur les commutateurs Catalyst CISCO

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-2002-AVI-017

Gestion du document

Référence	CERTA-2002-AVI-017
Titre	Vulnérabilité de `telnet` sur les commutateurs Catalyst CISCO
Date de la première version	30 janvier 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

Commutateurs CISCO Catalyst :

- série 6000 ;
- série 5000 ;
- série 4000 ;
- 2948G ;
- 2900.

3 Résumé

Une vulnérabilité dans le service `telnet` de ces commutateurs permet à un utilisateur mal intentionné de les redémarrer à volonté.

4 Description

Un débordement de mémoire dans `telnet` sous CatOs (système d'exploitation des Catalyst) permet à un utilisateur mal intentionné de redémarrer à distance le commutateur.

5 Contournement provisoire

- Filtrer le port 23/TCP (`telnet`) sur le garde barrière afin d'éviter une attaque provenant de l'extérieur.
- S'il n'est pas nécessaire, supprimer l'accès distant au commutateur par `telnet`.
- Si cela est possible, supprimer l'adresse IP du commutateur ainsi que toute forme d'administration distante de ce dernier.

6 Solution

Appliquer le correctif comme indiqué dans le bulletin de sécurité de CISCO :
http://www.cisco.com/

7 Documentation

- Le bulletin de sécurité de CISCO :
  http://www.cisco.com/warp/public/707/catos-telrcv-vuln-pub.shtml
- La vulnérabilité du démon `telnetd` avait déja fait l'objet d'un avis du CERTA : CERTA-2001-AVI-081-002.
- L'avis du CERTA faisait référence à l'avis de sécurité du CERT/CC :
  http://www.cert.org/advisories/CA-2001-21.html

Gestion détaillée du document

30 janvier 2002 version initiale.