Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 février 2001
N° CERTA-2001-AVI-013

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur les commutateurs CISCO série CSS

Gestion du document

Référence	CERTA-2001-AVI-013
Titre	Vulnérabilités sur les commutateurs CISCO série CSS
Date de la première version	05 février 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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 ;
- accès aux fichiers de configuration.

2 Systèmes affectés

- Cisco CSS 11050 ;
- Cisco CSS 11150 ;
- Cisco CSS 11800.

3 Résumé

Un utilisateur mal intentionné peut, par le biais d'une connection telnet, entraîner un déni de service ou visualiser les fichiers de configuration du commutateur cible.

4 Description

Les commutateurs CISCO de la série 11000 peuvent être configurés pour que l'accès telnet soit restreint ou complet.

Dans le cas d'un accès restreint, un utilisateur non authentifié (dont le compte n'est pas connu par le commutateur) peut par le biais d'une requête sur un nom de fichier trop long (débordement de pile) entraîner un blocage du commutateur.

Dans le cas d'une configuration en accès complet, la même vulnérabilité permet de visualiser certains fichiers de configuration ainsi que la structure des répertoires du commutateur.

5 Solution

Les mises à jour ainsi que les modifications à effectuer sont disponibles sur le site CISCO :
http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/bsccfggd/profiles.htm
http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/advcfggd/sgacleql.htm

6 Documentation

Bulletin de sécurité CISCO :
http://www.cisco.com/warp/public/707/arrowpoint-cli-filesystem-pub.shtml

Gestion détaillée du document

05 février 2001 version initiale.