Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 mars 2001
N° CERTA-2001-AVI-040

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les concentrateurs CISCO VPN3000

Gestion du document

Référence	CERTA-2001-AVI-040
Titre	Vulnérabilité dans les concentrateurs CISCO VPN3000
Date de la première version	29 mars 2001
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

Déni de service.

2 Systèmes affectés

Concentrateurs CISCO VPN3000 possédant une version logicielle inférieure à 3.0.00.
Cette série inclue les modèles 3005, 3015, 3030, 3060, et 3080.

3 Résumé

Un utilisateur distant mal intentionné peut, par l'envoi de multiples requêtes malformées, engendrer un déni de service obligeant le concentrateur à redémarrer.

4 Description

Le service telnet/SSL (port 992/tcp) et le port telnet standard (port 23/tcp) des concentrateurs de la série VPN3000 ne mettent pas fin à la connexion après la réception de requêtes malformées sur leurs ports.

Si un utilisateur distant mal intentionné « inonde » ces ports de fausses requêtes, le concentrateur ne peut plus interpréter les demandes entraînant un redémarrage du système.

5 Contournement provisoire

Par défaut ces deux services ne sont pas activés uniquement sur l'interface externe. Désactiver ces services dans vos configurations pour toutes les interfaces.

6 Solution

Un correctif est disponible sur le site CISCO :
http://www.cisco.com

7 Documentation

Avis Cisco :
http://www.cisco.com/warp/public/707/vpn3k-telnet-vuln-pub.shtml

Gestion détaillée du document

29 mars 2001 version initiale.