



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 avril 2006
N° CERTA-2006-AVI-051-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur les concentrateurs VPN 3000 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-2006-AVI-051>

Gestion du document

Référence	CERTA-2006-AVI-051-001
Titre	Vulnérabilité sur les concentrateurs VPN 3000 CISCO
Date de la première version	27 janvier 2006
Date de la dernière version	28 avril 2006
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 à distance.

2 Systèmes affectés

– Cisco VPN 3000 concentrator versions 4.7.0 à 4.7.2.A

3 Description

Une vulnérabilité présente dans les concentrateurs VPN CISCO 3000 peut être exploitée par un utilisateur distant mal intentionné via l'envoi de paquet HTTP malicieusement construit pour réaliser un déni de service ou pour déconnecter des utilisateurs déjà connectés.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Site Internet CISCO :
<http://www.cisco.com>
- Bulletin de sécurité 20060126 du 26 janvier :
<http://www.cisco.com/warp/public/707/cisco-sa-20060126-vpn.shtml>
- Mises à jour CISCO :
<http://www.cisco.com/cgi-bin/tablebuild.pl/vpn3000-3des>
- Référence CVE CAN-2006-0483 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0483>

Gestion détaillée du document

27 janvier 2006 version initiale.

28 avril 2006 ajout de la référence CVE et de la référence aux correctifs CISCO.