Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 août 2006
N° CERTA-2006-AVI-369

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les concentrateurs Cisco VPN 3000

Gestion du document

Référence	CERTA-2006-AVI-369
Titre	Vulnérabilités dans les concentrateurs Cisco VPN 3000
Date de la première version	24 août 2006
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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

Concenctrateur Cisco VPN 3005, 3015, 3020, 3030, 3060 et 3080 versions
- antérieures à la version 4.1 ;
- 4.1.x antérieures à la version 4.1(7)M ;
- 4.7.x antérieures à la version 4.7(2)G.

3 Résumé

Deux vulnérabilités sont présentes dans les concentrateurs Cisco VPN 3000. Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné pour contourner certaines restrictions de sécurité.

4 Description

Deux vulnérabilités présentes sur plusieurs commandes FTP permettent à un utilisateur non authentifié d'exécuter ces commandes. Le protocole FTP, actif par défaut, est utilisé comme protocole de gestion de l'équipement.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).
Appliquer le correctif suivant disponible sur le site de l'éditeur :
http://www.cisco.com/pcgi-bin/tablebuild.pl/vpn3000-3des?psrtdcat20e2

6 Documentation

- Bulletin de sécurité Cisco du 23 août 2006 :
  http://www.cisco.com/warp/public/707/cisco-sa-20060823-vpn3k.shtml

Gestion détaillée du document

version initiale.