

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur le client VPN 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-205>

Gestion du document

Référence	CERTA-2002-AVI-205
Titre	Vulnérabilités sur le client VPN Cisco
Date de la première version	09 septembre 2002
Date de la dernière version	–
Source(s)	Avis 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 ;
- divulgation d'informations ;

2 Systèmes affectés

Client VPN Cisco sur les plates-formes suivantes :

- Windows ;
- Linux utilisant une version du noyau équivalente ou supérieure à la version 2.2.12 exceptée la version 2.5 ;
- Solaris UltraSPARC sur les architectures 32 bits et 64 bits utilisant une version du noyau 2.6 ou supérieure ;
- Mac OS X versions 10.1.0 ou supérieures.

3 Résumé

Le client VPN Cisco est une application chargée d'établir des connexions sur un réseau privé virtuel pour des communications chiffrées et authentifiées.

Plusieurs vulnérabilités ont été découvertes sur les clients VPN Cisco.

4 Description

Le numéro des vulnérabilités ci-dessous correspond à l'identification Cisco :

- CSCdt35749 : les clients VPN qui reçoivent des paquets TCP spécifiques ayant comme ports source et destination le port 137 (NETBIOS Name Service) sont vulnérables à une attaque par déni de service.
- CSCdt60391 : sur les plates-formes Windows, un utilitaire permet de découvrir les mots de passe chiffrés du groupe IPSEC ;
- CSCdw87717 : une vulnérabilité dans le processus d'authentification du serveur par le client permet à un utilisateur mal intentionné de réaliser une attaque du type « Man in the middle » ;
- CSCdy37058 : une vulnérabilité du client VPN permet à un utilisateur mal intentionné d'envoyer un paquet sur le réseau privée virtuel. Cette vulnérabilité n'est exploitable que si la fonction `split tunneling` est désactivée.

5 Solution

Appliquer les correctifs correspondant à votre plate-forme (cf. section documentation).

6 Documentation

- Procédure de mise à jour du client VPN Cisco :
<http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/>
- Correctifs :
<http://www.cisco.com/kobayashi/sw-center/vpn/client/>
- Avis de sécurité de Cisco :
<http://www.cisco.com/warp/public/707/vpnclient-multiple2-vuln-pub.shtml>

Gestion détaillée du document

09 septembre 2002 version initiale.