



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 septembre 2002
N° CERTA-2002-AVI-212

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du client VPN 5000 de 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-212>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2002-AVI-212 |
| Titre | Multiples vulnérabilités du client VPN 5000 de Cisco |
| Date de la première version | 19 septembre 2002 |
| 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

Elévation de privilèges.

2 Systèmes affectés

- Client VPN 5000 sur Linux et Solaris ;
- client VPN sur MacOS.

3 Résumé

Il existe un débordement de mémoire dans les clients VPN 5000 de Cisco permettant d'obtenir les privilèges de l'administrateur `root` sous Linux et Solaris.

Il est également possible d'obtenir le dernier mot de passe tapé sur un client VPN 5000 sous MacOS.

4 Description

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

Une vulnérabilité de type débordement de mémoire présente dans les commandes `close_tunnel` et `open_tunnel` permet à un utilisateur mal intentionné d'obtenir les privilèges de l'administrateur `root`.

D'autre part, il est possible sur les clients MacOs de lire le dernier mot de passe entré stocké en clair sur la machine.

5 Solution

Consulter le bulletin de sécurité de Cisco (voir paragraphe Documentation) pour connaître la disponibilité des mises à jour.

6 Documentation

Bulletin de sécurité de Cisco «Cisco VPN 5000 client buffer overflow vulnerabilities»:
<http://cisco.com/warp/public/707/vpn5k-client-multiple-vuln-pub.html>

Gestion détaillée du document

19 septembre 2002 version initiale.