

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du client VPN 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-131>

Gestion du document

Référence	CERTA-2002-AVI-131
Titre	Vulnérabilité du client VPN de Cisco
Date de la première version	20 juin 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité de CISCO "Buffer overflow in UNIX VPN Client"
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 ;
- exécution de code arbitraire.

2 Systèmes affectés

Cisco VPN Clients versions 3.5.1 et précédentes pour Linux, Solaris et Mac OS X.

3 Résumé

Un individu mal intentionné peut exécuter du code arbitraire en local avec les privilèges de l'administrateur.

4 Description

Le client VPN (Virtual Private Network) CISCO permet d'établir un tunnel chiffré entre le système local et un concentrateur VPN CISCO. Le tunnel fournit alors une confidentialité et une intégrité des données transmises, permettant à un utilisateur de se connecter à un réseau d'entreprise à travers un réseau public.

Une vulnérabilité présente dans le client VPN CISCO peut être exploitée par un individu mal intentionné possédant un compte local sur le système afin d'exécuter du code arbitraire avec les privilèges de l'administrateur.

5 Contournement provisoire

Par défaut, l'installation du fichier binaire s'effectue avec les permissions `setuid`. Il est possible de minimiser la vulnérabilité en supprimant les droits `setuid` sur le binaire permettant l'exécution du client VPN avec la commande suivante :

```
/bin/chmod 755 /usr/local/bin/vpnclient
```

6 Solution

Installer la version 3.5.2 du client VPN de CISCO disponible chez CISCO :
<http://www.cisco.com>

7 Documentation

Bulletin de sécurité CISCO "Buffer overflow in UNIX VPN Client" :
<http://www.cisco.com/warp/public/707/cisco-unix-vpnclient-buffer-overflow-pub.shtml>

Gestion détaillée du document

20 juin 2002 version initiale.