



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 mai 2006
N° CERTA-2006-AVI-139-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'OpenVPN

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-139>

Gestion du document

Référence	CERTA-2006-AVI-139-002
Titre	Vulnérabilité d'OpenVPN
Date de la première version	06 avril 2006
Date de la dernière version	04 mai 2006
Source(s)	Bulletin de sécurité du site OpenVPN
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Les versions OpenVPN 2.0 à 2.0.5.

3 Résumé

Une vulnérabilité permet à un utilisateur malveillant de forcer la configuration d'un client OpenVPN et de lancer des commandes arbitraires à distance.

4 Description

OpenVPN est un système client-serveur. Un utilisateur malveillant ayant compromis le serveur peut modifier la configuration d'un client au moyen de la commande `setenv`. Il peut aussi profiter de cette propriété pour lancer un code malveillant à l'insu du client et donc exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Site officiel du projet OpenVPN, mises à jour :
<http://openvpn.net>
- Référence au bulletin de sécurité Mandriva MDKSA-2006:069 du 10 avril 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MKDSA-2006:069>
- Référence au bulletin de sécurité Debian DSA-1045 du 27 avril 2006 :
<http://www.debian.org/security/2006/dsa-1045>
- Bulletin de sécurité SUSE SUSE-SR:2006:009 du 28 avril 2006 :
http://www.novell.com/linux/security/advisories/2006_04_28.html
- Référence CVE CVE-2006-1629 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1629>

Gestion détaillée du document

06 avril 2006 version initiale.

11 avril 2006 ajout de la référence au bulletin de sécurité Mandriva.

04 mai 2006 ajout des références aux bulletins de sécurité Debian et SUSE.