



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-183

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-183>

Gestion du document

Référence	CERTA-2006-AVI-183
Titre	Vulnérabilités dans OpenVPN
Date de la première version	04 mai 2006
Date de la dernière version	–
Source(s)	
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

OpenVPN versions 2.0.7 et précédentes.

3 Résumé

Une vulnérabilité dans OpenVPN permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire à partir de l'interface d'administration à distance.

4 Description

La vulnérabilité est causée par une mauvaise conception (qui ne serait pas activée par défaut) dans l'interface d'administration à distance d'OpenVPN. Cette vulnérabilité permet d'accéder à cette interface sans aucune authentification préalable et ceci à partir du réseau local ou bien à partir de l'Internet.

5 Solution

Dans l'attente d'un correctif de la part de l'éditeur, il est recommandé d'interdire l'administration à distance à partir d'Internet mais aussi à partir d'un réseau local. N'autoriser cette administration qu'à partir d'une machine dédiée bénéficiant d'un contrôle d'accès.

Gestion détaillée du document

04 mai 2006 version initiale.