

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans la série des commutateurs CISCO VPN 3000

---

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-2003-AVI-082>

---

### Gestion du document

Référence	CERTA-2003-AVI-082
Titre	Vulnérabilités dans la série des commutateurs CISCO VPN 3000
Date de la première version	12 mai 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO : "Cisco VPN 3000 Concentrator Vulnerabilities"
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

- Contournement de la politique de sécurité ;
- déni de service.

## 2 Systèmes affectés

- La série des commutateurs Cisco VPN 3000 ;
- Cisco VPN 3002 Hardware Client.

## 3 Résumé

Trois vulnérabilités présentes dans la série des commutateurs Cisco VPN 3000 permettent à un utilisateur mal intentionné d'effectuer un déni de service sur le commutateur ou de contourner la politique de sécurité.

## 4 Description

- L'utilisation d'un tunnel IPSEC avec TCP permet dans certains cas d'accéder à des machines d'un réseau local lorsqu'elles utilisent le même port de communication que celui utilisé par le tunnel.

- Une vulnérabilité présente dans le service SSH permet le redémarrage du commutateur lors de l'envoi de paquets malicieusement construits.
- L'envoi de paquets malicieux ICMP sur l'une des interfaces du commutateur permet d'effectuer un déni de service ou d'en dégrader les performances.

## **5 Solution**

Appliquer les correctifs fournis par CISCO :

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/>

## **6 Documentation**

Bulletin de sécurité CISCO : "Cisco VPN 3000 Concentrator Vulnerabilities"

<http://www.cisco.com/warp/public/707/cisco-sa-20030507-vpn3k.shtml>

## **Gestion détaillée du document**

**12 mai 2003** version initiale.