

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité des équipements Cisco VPN Concentrator

---

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-2005-AVI-125>

---

### Gestion du document

Référence	CERTA-2005-AVI-125
Titre	Vulnérabilité des équipements Cisco VPN Concentrator
Date de la première version	31 mars 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #64347 du 30 mars 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

Déni de service.

## 2 Systèmes affectés

Cisco VPN 3000 Series Concentrators fonctionnant sous la version 4.1.7.A ou versions antérieures.

## 3 Résumé

Une vulnérabilité découverte dans les équipements Cisco VPN 3000 permet à un utilisateur mal intentionné présent sur le réseau local d'effectuer un déni de service.

## 4 Description

Une vulnérabilité causée par un mauvais traitement du protocole SSL permet à un individu malveillant d'effectuer un déni de service à partir du réseau local, au moyen de paquets HTTPS malicieusement constitués.

Cette vulnérabilité est exploitable uniquement si le service HTTPS est activé.

## **5 Solution**

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

## **6 Documentation**

- Site Internet de l'éditeur :  
<http://www.cisco.com>
- Bulletin de sécurité Cisco #64347 du 30 mars 2005 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20050330-vpn3k.shtml>

## **Gestion détaillée du document**

**31 mars 2005** version initiale.