

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité des IOS 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-2006-AVI-386>

---

### Gestion du document

Référence	CERTA-2006-AVI-386
Titre	Vulnérabilité des IOS Cisco
Date de la première version	08 septembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #71314 du 06 septembre 2006
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.

## 2 Systèmes affectés

- Cisco IOS 12.x ;
- Cisco IOS R12.x.

## 3 Résumé

Une vulnérabilité dans le système d'exploitation IOS des équipements Cisco permet à un utilisateur mal intentionné de contourner la politique de sécurité du système.

## 4 Description

Une erreur dans la mise en œuvre du protocole GRE (Generic Routine Encapsulation) par le système d'exploitation des équipements Cisco (IOS) permet à un utilisateur du réseau local de contourner la politique de sécurité définie dans les listes d'accès (*Access Control List* ou *ACL*) du système.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Cisco ID 71314 du 06 septembre 2006 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20060906-gre.shtml>

## **Gestion détaillée du document**

**08 septembre 2006** version initiale.