

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Cisco IOS

---

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-034>

---

### Gestion du document

Référence	CERTA-2006-AVI-034
Titre	Vulnérabilité de Cisco IOS
Date de la première version	19 janvier 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20060118-sgbp du 18 janvier 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

Déni de service.

## 2 Systèmes affectés

Cisco IOS versions 12.0, 12.1, 12.2, 12.3 et 12.4 avec le support du protocole SGBP activé.

## 3 Résumé

Une vulnérabilité du système d'exploitation Cisco IOS permet à un utilisateur mal intentionné de réaliser un déni de service.

## 4 Description

Cisco IOS est le système d'exploitation mis en oeuvre dans les routeurs Cisco. Dans le cas où le support pour le protocole SGBP est activé, un utilisateur mal intentionné peut bloquer le routeur vulnérable ou provoquer le redémarrage d'un routeur au moyen d'un datagramme UDP malicieusement constitué à destination du port 9900.

## **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 cisco-sa-20060118-sgbp du 18 janvier 2006 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>

## **Gestion détaillée du document**

**19 janvier 2006** version initiale.