

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités du module IPS 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-2007-AVI-089>

---

### Gestion du document

Référence	CERTA-2007-AVI-089
Titre	Multiples vulnérabilités du module IPS de Cisco IOS
Date de la première version	16 février 2007
Date de la dernière version	–
Source(s)	Bulletin Cisco du 13 février 2007
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 ;
- Contournement de la politique de sécurité.

## 2 Systèmes affectés

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

## 3 Résumé

Deux vulnérabilités concernent le module IPS des systèmes *Cisco IOS* affectés. Elles permettent respectivement de contourner la politique de sécurité et de provoquer un déni de service à distance.

## 4 Description

Le module IPS (*Intrusion protection system*) des systèmes *Cisco IOS* réagit aux intrusions qu'il détecte sur la base de signatures.

Deux vulnérabilités affectent les systèmes *IOS* lorsque le module IPS est activé :

- une mauvaise gestion des paquets fragmentés permet, dans certaines circonstances, de contourner le filtrage ;
- du trafic malveillant peut provoquer un déni de service par arrêt inopiné (*crash*) 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 81545 du 13 février 2007 :  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a00807e2484.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a00807e2484.shtml)

## **Gestion détaillée du document**

**16 février 2007** version initiale.