

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans CISCO IDS et CISCO IPS

---

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-405>

---

### Gestion du document

Référence	CERTA-2006-AVI-405
Titre	Vulnérabilités dans CISCO IDS et CISCO IPS
Date de la première version	21 septembre 2006
Date de la dernière version	–
Source(s)	
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 IDS versions 4.1 ;
- CISCO IPS versions 5.0 ;
- CISCO IPS versions 5.1.

## 3 Résumé

Des vulnérabilités ont été découvertes dans CISCO Intrusion Prevention System et dans CISCO Intrusion Detection System. Elles conduisent à un déni de service et au contournement de la politique de sécurité.

## **4 Description**

La vulnérabilité dans CISCO Intrusion Detection System est due à une erreur dans l'interface d'administration pour la partie relative à la gestion des paquets SSL mal formés. La vulnérabilité dans CISCO Intrusion Prevention System est due à une erreur dans le traitement des paquets IP fragmentés. Cette vulnérabilité pourrait être exploitée pour contourner la politique de sécurité.

## **5 Solution**

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

## **6 Documentation**

- Bulletins de sécurité de CISCO :  
<http://cisco.com/warp/public/707/cisco-sa-20060920-ips.shtml>

## **Gestion détaillée du document**

**21 septembre 2006** version initiale.