

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de la pile IPv6 des équipements 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-2005-AVI-309>

---

### Gestion du document

Référence	CERTA-2005-AVI-309
Titre	Vulnérabilité de la pile IPv6 des équipements Cisco
Date de la première version	11 août 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 65783 du 29 juillet 2005
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 ;
- Execution de code arbitraire à distance.

## 2 Systèmes affectés

La plupart des équipements Cisco qui disposent d'un IOS. Pour savoir si le système est affecté, se référer au bulletin de sécurité Cisco (cf. Documentation).

## 3 Description

Une vulnérabilité dans la mise en œuvre du protocole IPv6 des IOS Cisco permet à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire par le biais d'un paquet IPv6 malicieusement construit.

## 4 Contournement provisoire

Désactiver le support de l'IPv6 sur l'équipement.

## **5 Solution**

Se référer au bulletin de sécurité Cisco pour appliquer le correctif approprié (cf. Documentation).

## **6 Documentation**

- Bulletin de sécurité Cisco 65783 du 29 juillet 2005.  
<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>

## **Gestion détaillée du document**

**11 août 2005** version initiale.