

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité IPv6 dans 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-2005-AVI-032>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2005-AVI-032                                    |
| Titre                       | Vulnérabilité IPv6 dans Cisco IOS                     |
| Date de la première version | 27 janvier 2005                                       |
| Date de la dernière version | –   |
| Source(s)                   | Bulletin de sécurité CISCO n°63844 du 26 janvier 2005 |
| Pièce(s) jointe(s)          |   |

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

Cette vulnérabilité affecte tous les dispositifs Cisco fonctionnant sous le système d'exploitation IOS (Internet-work Operating System) dont le protocole IPv6 est activé.

## 3 Résumé

Une vulnérabilité découverte dans le système d'exploitation Cisco IOS permet à un utilisateur distant mal intentionné d'effectuer un déni de service sur le système vulnérable.

## 4 Description

Un utilisateur mal intentionné peut forcer à distance le redémarrage du dispositif vulnérable, ce qui se traduit par un déni de service. Cette vulnérabilité peut être exploitée au moyen de l'envoi de nombreux paquets IPv6 (Internet Protocol Version 6) malicieusement construits.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Cisco n° 63844 du 26 janvier 2005 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>

## **Gestion détaillée du document**

**27 janvier 2005** version initiale.