

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité les routeurs Cisco supportant MPLS

---

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-031>

---

### Gestion du document

Référence	CERTA-2005-AVI-031
Titre	Vulnérabilité les routeurs Cisco supportant MPLS
Date de la première version	27 janvier 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco du 26 janvier 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.

## 2 Systèmes affectés

L'ensemble des routeurs Cisco supportant MPLS (Cisco IOS version 12.1T, 12.2, 12.3 et 12.3T) :

- routeurs des séries 2600 et 2800 ;
- routeurs des séries 3600, 3700 et 3800 ;
- routeurs des séries 4500 et 4700 ;
- Access Servers séries 5300, 5350 et 5400.

## 3 Résumé

Une vulnérabilité dans le traitement des paquets MPLS (Multi Protocol Label Switching) permet à un utilisateur mal intentionné d'effectuer un déni de service sur les routeurs affectés par cette vulnérabilité.

## **4 Description**

MPLS (Multi Protocol Label Switching) est un protocole de routage réseau utilisé pour effectuer de la commutation rapide. Une vulnérabilité présente dans le traitement des paquets MPLS (Multi Protocol Label Switching) permet à un utilisateur mal intentionné d'effectuer un déni de service via l'envoi d'un paquet MPLS malicieux à une interface sur laquelle MPLS est désactivé.

## **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 "Crafted Packet Causes Reload on Cisco Routers" du 26 janvier 2005 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20052601-les.shtml>

## **Gestion détaillée du document**

**27 janvier 2005** version initiale.