

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Cisco IOS Line Printer Daemon

---

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-438>

---

### Gestion du document

Référence	CERTA-2007-AVI-438
Titre	Vulnérabilité dans Cisco IOS Line Printer Daemon
Date de la première version	12 octobre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco ID 99109 du 10 octobre 2007 Bulletin de sécurité IRM ID 024 du 10 octobre 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

## 2 Systèmes affectés

Toutes versions de Cisco IOS mettant en œuvre le service Line Printer Daemon.

*Remarque : le service lpd n'est pas activé par défaut.*

## 3 Résumé

Une vulnérabilité dans Cisco IOS permet à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

## 4 Description

Une vulnérabilité de type débordement de mémoire dans la fonction `sprintf()` du démon `Line Printer Daemon` peut être exploitée par une personne malveillante, au moyen d'un nom d'hôte spécialement construit, afin de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

## 5 Contournement provisoire

Un contournement provisoire est proposé par Cisco sur son bulletin de sécurité, disponible à l'adresse suivante : <http://www.cisco.com/warp/public/707/cisco-sr-20071010-lpd.shtml>

## 6 Solution

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

## 7 Documentation

- Bulletin de sécurité Cisco ID 99109 du 10 octobre 2007 :  
<http://www.cisco.com/warp/public/707/cisco-sr-20071010-lpd.shtml>
- Bulletin de sécurité IRM ID 024 du 10 octobre 2007 :  
<http://www.irmplc.com/index.php/155-Advisory-024>

## Gestion détaillée du document

12 octobre 2007 version initiale.