

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Faille dans le système d'impression lpr

---

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-2003-AVI-046>

---

### Gestion du document

Référence	CERTA-2003-AVI-046-002
Titre	Faille dans le système d'impression lpr
Date de la première version	14 mars 2003
Date de la dernière version	22 mai 2003
Source(s)	-
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

Elévation de privilèges en local.

## 2 Systèmes affectés

Systèmes Unix suivants :

- OpenBSD jusqu'à 3.2 ;
- SuSE Linux jusqu'à 7.3 ;
- Debian Linux versions 2.2 et 3.0 ;
- Mandrake Linux jusqu'à 8.2.

## 3 Résumé

Une faille dans la commande *lprm* permet à un utilisateur local d'obtenir les droits avec lesquels s'exécute la commande (*root* ou utilisateur privilégié *daemon*).

## 4 Description

Un débordement de mémoire dans le programme *lprm* (suppression d'un travail d'impression dans la file d'attente) permet d'injecter du code arbitraire qui sera alors exécuté avec des privilèges élevés, le binaire ayant les droits *root* ou *daemon*.

## 5 Contournement provisoire

Supprimer les droits "suid" de la commande *lprm* en l'absence de correctif (son usage sera alors restreint).

## 6 Solution

Appliquer le correctif de l'éditeur :

- OpenBSD :  
<http://www.openbsd.org/errata.html>
- SuSE Linux :  
[http://www.suse.com/de/security/2003\\_014\\_lprold.html](http://www.suse.com/de/security/2003_014_lprold.html)
- Debian Linux :  
<http://www.debian.org/security/2003/dsa-267>
- Mandrake Linux :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:059>

## 7 Documentation

Référence CVE CAN-2003-0144 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0144>

## Gestion détaillée du document

**14 mars 2003** version initiale.

**25 mars 2003** ajout de la distribution Debian et de la référence CVE.

**22 mai 2003** ajout de la distribution Mandrake.