

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans cdrecord

---

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-089>

---

### Gestion du document

Référence	CERTA-2003-AVI-089
Titre	Vulnérabilité dans cdrecord
Date de la première version	19 mai 2003
Date de la dernière version	–
Source(s)	–
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

Elévation de privilèges.

## 2 Systèmes affectés

cdrecord version 2.0.

## 3 Résumé

Un débordement de tampon dans le logiciel cdrecord permet de réaliser une élévation de privilèges et d'obtenir les droits du super-utilisateur (root).

## 4 Description

cdrecord est un logiciel de gravure sous GNU/Linux s'exécutant avec les privilèges de l'administrateur. Un débordement de tampon dans la variable dev permet à un utilisateur mal intentionné de procéder à une élévation de privilèges et d'obtenir les droits du super-utilisateur (root).

## **5 Solution**

Mettre à jour selon la distribution concernée (cf. section Documentation).

## **6 Documentation**

- Référence CVE CAN-2003-0289 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0289>
- Avis de sécurité Mandrake MDKSA-2003:058 :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:068>

## **Gestion détaillée du document**

**19 mai 2003** version initiale.