



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 22 février 2005
N° CERTA-2004-AVI-303-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2004-AVI-303>

Gestion du document

Référence	CERTA-2004-AVI-303-002
Titre	Vulnérabilité de cdrecord
Date de la première version	08 septembre 2004
Date de la dernière version	22 février 2005
Source(s)	Bulletin de sécurité Mandrake MDKSA-2004:091 du 07 septembre 2004
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 2.00.3 et versions antérieures.

3 Description

cdrecord est un logiciel de gravure pour UNIX s'exécutant avec les privilèges de l'administrateur. Une vulnérabilité dans cdrecord permet à un utilisateur mal intentionné d'élever ses privilèges et de devenir super-utilisateur root.

4 Solution

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

5 Documentation

- Site Internet de cdrecord :
<http://www.fokus.fhg.de/research/cc/glone/employees/joerg.schilling/private/cdrecord.html>
- Bulletin de sécurité Mandrake MDKSA-2004:091 du 07 septembre 2004 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:091>
- Bulletin de sécurité Gentoo GLSA 200409-18 du 14 septembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200409-18.xml>
- Bulletin de sécurité Fedora FLSA:2058 du 20 février 2005 :
https://bugzilla.fedora.us/show_bug.cgi?id=2058
- Référence CVE CAN-2004-0806 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0806>

Gestion détaillée du document

08 septembre 2004 version initiale.

15 septembre 2004 ajout référence au bulletin de sécurité de Gentoo.

22 février 2005 ajout référence au bulletin de sécurité de Fedora.