



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 janvier 2006
N° CERTA-2006-AVI-006-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans cpio

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-2006-AVI-006>

Gestion du document

Référence	CERTA-2006-AVI-006-001
Titre	Vulnérabilité dans cpio
Date de la première version	04 janvier 2006
Date de la dernière version	12 janvier 2006
Source(s)	Bulletin de sécurité Ubuntu USN-234 du 02 janvier 2006
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

cpio 2.x.

3 Résumé

Une vulnérabilité dans cpio permet à un utilisateur local mal intentionné de provoquer un déni de service.

4 Description

cpio est un logiciel libre permettant la création et la manipulation d'archives.

Une vulnérabilité de type débordement de mémoire dans la fonction `write_out_header()` peut être exploitée par un utilisateur mal intentionné afin de provoquer un déni de service.

5 Solution

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

6 Documentation

- Bulletin de sécurité Ubuntu USN-234-1 du 02 janvier 2006 :
<http://www.ubuntulinux.org/usn/usn-234-1>
- Bulletin de sécurité Mandriva MDKSA-2005:237 du 23 décembre 2005 :
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:237>
- Bulletin de sécurité FreeBSD du 11 janvier 2006 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:03.cpio.asc>
- Référence CVE CAN-2005-4268 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-4268>

Gestion détaillée du document

04 janvier 2006 version initiale.

12 janvier 2006 ajout des références aux bulletins de sécurité FreeBSD et Mandriva.