

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de 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-2005-AVI-251>

---

### Gestion du document

Référence	CERTA-2005-AVI-251-003
Titre	Vulnérabilité de cpio
Date de la première version	12 juillet 2005
Date de la dernière version	10 octobre 2005
Source(s)	Bulletin de sécurité Mandriva MDKSA-2005:116 du 11 juillet 2005
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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données.

## 2 Systèmes affectés

cpio version 2.6 et versions antérieures.

## 3 Description

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

Deux vulnérabilités dans cpio permettent à un utilisateur local mal intentionné de modifier des permissions de fichiers du système vulnérable (CAN-2005-1111) et à un utilisateur distant mal intentionné, au moyen d'une archive habilement constituée, d'écrire dans des répertoires arbitraires du système vulnérable (CAN-2005-1229).

## 4 Solution

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

## 5 Documentation

- Site Internet de GNU `cpio` :  
<http://www.gnu.org/software/cpio/cpio.html>
- Bulletin de sécurité Mandriva MDKSA-2005:116 du 11 juillet 2005 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:116>
- Bulletin de sécurité Mandriva MDKSA-2005:116-1 du 19 juillet 2005 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:116-1>
- Bulletin de sécurité RedHat RHSA-2005:378 du 21 juillet 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-378.html>
- Bulletin de sécurité Debian DSA-846 du 07 octobre :  
<http://www.debian.org/security/2005/dsa-846>
- Référence CVE CAN-2005-1111 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1111>
- Référence CVE CAN-2005-1229 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1229>

### Gestion détaillée du document

**12 juillet 2005** version initiale.

**20 juillet 2005** ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:116-1.

**22 juillet 2005** ajout de la référence au bulletin de sécurité RedHat RHSA-2005:378.

**10 octobre 2005** ajout de la référence au bulletin de sécurité Debian DSA-846.