

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de zip

---

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-391>

---

### Gestion du document

Référence	CERTA-2004-AVI-391-002
Titre	Vulnérabilité de zip
Date de la première version	10 décembre 2004
Date de la dernière version	06 janvier 2005
Source(s)	Bulletin de sécurité Hexview du 03 novembre 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

- Déni de service ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

Zip version 2.3 et versions antérieures.

## 3 Résumé

Une vulnérabilité de type débordement de mémoire dans l'utilitaire Zip permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

Zip est un outil de décompression d'archives au format zip. Lors d'une décompression récursive d'un répertoire, la taille du chemin résultant n'est pas correctement validée. Ceci permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance au moyen d'une archive malicieusement construite.

## 5 Solution

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

## 6 Documentation

- Site Internet de Zip :  
<http://www.info-zip.org/Zip.html>
- Bulletin de sécurité Hexview du 03 novembre 2004 :  
<http://www.hexview.com/docs/20041103-1.txt>
- Bulletin de sécurité Gentoo GLSA 200411-16 du 09 novembre 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200411-16.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:141 du 25 novembre 2004 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:141>
- Bulletin de sécurité Red Hat RHSA-2004:634 du 16 décembre 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-634.html>
- Bulletin de sécurité Debian DSA-624 du 05 janvier 2005 :  
<http://www.debian.org/security/2005/dsa-624>
- Bulletin de sécurité FreeBSD pour zip du 01 décembre 2004 :  
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité OpenBSD pour zip du 04 décembre 2004 :  
<http://www.vuxml.org/openbsd/>
- Référence CVE CAN-2004-1010 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1010>

## Gestion détaillée du document

**10 décembre 2004** version initiale.

**20 décembre 2004** ajout référence au bulletin de sécurité de Red Hat.

**06 janvier 2005** ajout référence au bulletin de sécurité de Debian.