

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités de gzip

---

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-2002-AVI-019>

---

### Gestion du document

Référence	CERTA-2002-AVI-019
Titre	Vulnérabilités de gzip
Date de la première version	01 février 2002
Date de la dernière version	–
Source(s)	Avis de Sécurité Mandrake MDKSA-2002:011
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 ;
- élévation de privilèges.

## 2 Systèmes affectés

Utilitaire *gzip* version 1.2.4.

## 3 Résumé

Deux vulnérabilités de *gzip* permettent à un utilisateur mal intentionné de provoquer un déni de service ou d'élérer ses privilèges.

## 4 Description

L'utilitaire *gzip* est utilisé pour la compression.  
Deux vulnérabilités sont présentes dans *gzip*.

La première provoque un déni de service si le fichier en entrée possède un nom supérieur à 1020 caractères.  
La deuxième vulnérabilité est un dépassement de mémoire qui peut être exploitée si *gzip* est utilisé sur un serveur (un serveur FTP par exemple).

## **5 Solution**

Contactez votre éditeur pour obtenir une mise à jour. Un correctif est disponible sur le site de *gzip* (cf. Documentation).

## **6 Documentation**

- Avis de sécurité Mandrake MDKSA-2002:011 :  
<http://www.linux-mandrake.com/en/security/2002/MDKSA-2002-011.php>
- Site de *gzip* :  
<http://www.gzip.org>

## **Gestion détaillée du document**

**01 février 2002** version initiale.