



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 08 février 2007  
N° CERTA-2007-AVI-072

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans WinRAR et RAR

---

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-2007-AVI-072>

---

### Gestion du document

Référence	CERTA-2007-AVI-072
Titre	Vulnérabilité dans WinRAR et RAR
Date de la première version	08 février 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDefense du 07 février 2007
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

Exécution de code arbitraire.

## 2 Systèmes affectés

- WinRAR 3.61 sous Microsoft Windows ;
- RAR 3.60 sur Linux.

D'autres versions peuvent être affectées.

## 3 Résumé

Une vulnérabilité dans *Unrar* permettrait à une personne malintentionnée d'exécuter du code arbitraire avec les privilèges de la personne ouvrant le fichier.

## 4 Description

*Unrar* est un outil en ligne de commande permettant de décompresser des fichiers sur Windows et Linux. Il fait partie des applications *WinRAR* et *RAR* de ces systèmes.

Une vulnérabilité de type débordement de mémoire dans *Unrar* permettrait à un attaquant d'exécuter du code arbitraire avec les privilèges de l'utilisateur qui tente de décompresser le fichier malveillant. Ceci est provoqué par une mauvaise interprétation de certains mots de passe.

Cette vulnérabilité ne concerne pas l'utilisation de *WinRAR* en mode graphique sur Windows.

## 5 Solution

Se référer au site de l'éditeur pour l'obtention des mises à jour (cf. section Documentation). La vulnérabilité est corrigée dans les versions 3.70 beta de *WinRAR* et *RAR*.

## 6 Documentation

- Site de l'éditeur :  
<http://www.rarlabs.com/download.htm>
- Bulletin de sécurité iDefense du 07 février 2007 :  
<http://www.iddefense.com/application/poi/display?id=472>

## Gestion détaillée du document

08 février 2007 version initiale.