

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de WinRAR

---

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-393>

---

### Gestion du document

Référence	CERTA-2005-AVI-393-001
Titre	Multiples vulnérabilités de WinRAR
Date de la première version	11 octobre 2005
Date de la dernière version	21 novembre 2005
Source(s)	Liste des changements dans WinRAR 3.51
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 versions 3.50 et antérieures.

## 3 Résumé

Deux vulnérabilités dans WinRAR permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

Deux vulnérabilités sont présentes dans WinRAR :

- une erreur dans la mise en œuvre de l'affichage de la fenêtre de diagnostic lors d'un décodage de fichier au format UUE ou XXE permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'un fichier encodé en UUE ou en XXE malicieusement construit ;

- une erreur dans la mise en œuvre de la décompression des fichiers de type ACE permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'un fichier ACE malicieusement constitué.

## **5 Solution**

Mettre à jour WinRAR en version 3.51 :

<http://www.rarlabs.com/download.htm>

## **6 Documentation**

- Site de l'éditeur :  
<http://www.rarlabs.com>
- Liste des changements dans la version 3.51 :  
<http://www.rarlabs.com/rarnew.htm>
- Bulletin de sécurité Gentoo GLSA 200511-10 du 13 novembre 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200511-10.xml>

## **Gestion détaillée du document**

**11 octobre 2005** version initiale.

**21 novembre 2005** ajout de la référence au bulletin de sécurité Gentoo.