



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 29 mai 2007  
N° CERTA-2007-AVI-232

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités d'Antivir

---

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-232>

---

### Gestion du document

Référence	CERTA-2007-AVI-232
Titre	Multiples vulnérabilités d'Antivir
Date de la première version	29 mai 2007
Date de la dernière version	–
Source(s)	Article Avira du 23 mai 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 à distance ;
- déni de service à distance.

## 2 Systèmes affectés

- *Avira Antivir Personal Edition Classic 7.x* ;
- *Avira Antivir Personal Edition Premium 7.x* ;
- *Avira Antivir Premium Security suite 7.x* ;
- *Avira Antivir Server 6.x* ;
- *Avira Antivir Unix Mailgate 2.x* ;
- *Avira Antivir Workstation 7.x*.

## 3 Résumé

Plusieurs vulnérabilités dans le traitement de dossiers archives par l'antivirus *Avira Antivir* permettent à un utilisateur malveillant de provoquer un déni de service à distance ou d'exécuter un code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités dans le traitement de dossiers archives existent dans l'antivirus *Avira Antivir* :

- le traitement des fichiers de type LZH peut provoquer un débordement de mémoire (*buffer overflow*). Ce débordement est exploitable par un utilisateur malintentionné pour exécuter un code arbitraire à distance ;
- le traitement des fichiers de type UPX peut provoquer une division par zéro et provoquer l'arrêt inopiné (*crash*) du programme. Par le biais d'un fichier UPX spécialement conçu, un utilisateur malveillant peut provoquer un déni de service à distance ;
- le traitement des fichiers de type TAR peut provoquer une boucle infinie. Par le biais d'un fichier TAR spécialement conçu, un utilisateur malveillant peut provoquer un déni de service à distance.

## 5 Solution

La version 7.03.00.09 du composant *AVPack* et la version 7.04.00.24 du composant *Engine* corrigent le problème. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Article du forum Avira du 23 mai 2007 :  
<http://forum.antivir-pe.de/thread.php?threadid=22528>

## Gestion détaillée du document

29 mai 2007 version initiale.