

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Avast!

---

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-2006-AVI-392>

---

## Gestion du document

Référence	CERTA-2006-AVI-392
Titre	Vulnérabilités dans Avast!
Date de la première version	14 septembre 2006
Date de la dernière version	–
Source(s)	
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.

## 2 Systèmes affectés

- avast! Home et Professional Edition versions 4x;
- avast! Server Edition versions 4x.

## 3 Résumé

Des vulnérabilités affectent l'antivirus avast!. Ces vulnérabilités peuvent être exploitées par des agresseurs pour compromettre les machines vulnérables.

## 4 Description

Ces vulnérabilités sont dues à des failles dans la gestion des archives. Ainsi, une archive malicieusement construite pourrait permettre l'exécution de code arbitraire à distance.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

## **6 Documentation**

- Bulletin de Secunia :  
<http://secunia.com/advisories/21794>
- Référence CVE CAN-2006-4626 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-4626>

## **Gestion détaillée du document**

**14 septembre 2006** version initiale.