

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2007-AVI-516>

Gestion du document

Référence	CERTA-2007-AVI-516-002
Titre	Vulnérabilité dans avast!
Date de la première version	05 décembre 2007
Date de la dernière version	11 décembre 2007
Source(s)	Bulletin de sécurité avast! du 04 décembre 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.

2 Systèmes affectés

avast! 4 Home/Professional versions antérieures à 4.7.1098.

3 Résumé

Une vulnérabilité dans *avast! 4 Home/Professional* permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité a été découverte dans *avast! 4 Home/Professional* lors du traitement d'archives au format TAR. Un utilisateur malintentionné peut, par le biais d'une archive TAR spécifiquement constituée, exécuter du code arbitraire à distance.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité avast! du 04 décembre 2007 :
http://www.avast.com/eng/avast-4-home_pro-revision-history.html
- Téléchargement de la dernière version d'avast! :
<http://www.avast.com/eng/download.html>
- Référence CVE CVE-2007-6265 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6265>

Gestion détaillée du document

05 décembre 2007 version initiale.

06 décembre 2007 Révision du risque, du résumé et de la description.

11 décembre 2007 Ajout de la référence CVE.