

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de plusieurs produits de sécurité

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-212>

Gestion du document

Référence	CERTA-2007-AVI-212
Titre	Vulnérabilité de plusieurs produits de sécurité
Date de la première version	09 mai 2007
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

Déni de service à distance.

2 Systèmes affectés

- Avast! home/professionnal 4.x ;
- Avira Antivir ;
- Barracuda Spam Firewall ;
- Panda Antivirus Platinum 6.x et 7.x, Titanium, Entreprise Suite et Small Business Edition.

3 Résumé

Une vulnérabilité dans la gestion des archives au format zoo permet à un utilisateur malveillant de réaliser un déni de service à distance.

4 Description

Une vulnérabilité dans la gestion des archives au format zoo peut conduire à une boucle infinie et la consommation de toute la ressource processeur. Elle permet à un utilisateur malveillant de réaliser un déni de service à distance.

5 Solution

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

Pour *Avast!*, migrer en version 4.7.981 ou ultérieure.

Pour *Avira*, migrer la bibliothèque `avpack32.dll` en version 7.3.0.6. La société annonce avoir corrigé la vulnérabilité de 22 mars 2007.

Pour *Barracuda*, migrer en *firmware* 3.4 ou ultérieur et en version de définition de virus 2.0.6399 ou ultérieure.

Pour *Panda*, la société annonce que la mise à jour corrigeant la vulnérabilité est automatique. Le correctif date du 02 avril 2007.

6 Documentation

- Bulletin de sécurité *Barracuda* du 04 mai 2007 :
http://www.barracudanetworks.com/ns/resources/tech_alert.php
- Bulletin de version *Avast* du 30 avril 2007 :
http://www.avast.com/eng/avast-4-home_pro-revision-history.html
- Référence CVE CVE-2007-1669 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1669>
- Référence CVE CVE-2007-1670 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1670>
- Référence CVE CVE-2007-1671 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1669>
- Référence CVE CVE-2007-1672 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1672>

Gestion détaillée du document

09 mai 2007 version initiale.