Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mai 2007
N° CERTA-2007-AVI-235

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Avast! Antivirus

Gestion du document

Référence	CERTA-2007-AVI-235
Titre	Vulnérabilités dans Avast! Antivirus
Date de la première version	30 mai 2007
Date de la dernière version	–
Source(s)	Annonces de vulnérabilités nruns AG 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

- les versions d'Avast! antérieures à 4.7.700.

3 Description

Deux vulnérabilités ont été identifiées dans les produits de sécurité Avast! Antivirus. Ils ne manipuleraient pas correctement des fichiers compressés de format `CAB` (pour *Cabinet*) ou `SIS` (*Symbian Installation System*), pouvant provoquer un débordement de la pile. Une personne malveillante pourrait ainsi construire des documents spécialement conçus ; lorsque ceux-ci seront analysés par l'outil de sécurité, des commandes arbitraires pourraient ainsi être exécutées sur le système vulnérable.

4 Solution

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

5 Documentation

- Site officiel d'Avast! :
  http://www.avast.com
- Référence CVE CVE-2007-2845 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2845
- Référence CVE CVE-2007-2846 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2846
- Avis de sécurité nruns SA-2007.008 du 23 mai 2007 :
  http://www.nruns.com/parsing-engines-advisories.php
- Archive de Neohapsis publié le 24 mai 2007 :
  http://archives.neohapsis.com/archives/fulldisclosure/2007-05/0448.html

Gestion détaillée du document

30 mai 2007 version initiale.