

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités de Sophos Anti-Virus

---

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-541>

---

### Gestion du document

Référence	CERTA-2006-AVI-541
Titre	Vulnérabilités de Sophos Anti-Virus
Date de la première version	11 décembre 2006
Date de la dernière version	–
Source(s)	Article Sophos 21681 du 08 décembre 2006
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- Sophos Anti-Virus version 6.0.5 ainsi que celles antérieures ;
- Sophos Anti-Virus version 4.11 ainsi que celles antérieures.

## 3 Description

Plusieurs vulnérabilités ont été identifiées dans le produit Sophos Anti-Virus. Certaines concernant les fichiers aux formats RAR et CHM ont déjà été abordées dans l'avis du CERTA CERTA-2006-AVI-472 du 02 novembre 2006. Cependant, deux nouvelles vulnérabilités ont été publiquement annoncées :

- une mauvaise interprétation de certains fichiers d'archivage CPIO permettrait, sous certaines conditions, l'exécution de code arbitraire sur le système possédant une version vulnérable ;

- certaines chaînes de caractères dans les fichiers au format SIT (pour *Stuffit archives*) ne seraient pas correctement manipulées. Un fichier construit de manière malveillante pourrait donc exploiter cette vulnérabilité pour exécuter du code arbitraire 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

- Avis Sophos concernant les vulnérabilités communiquées par iDefense, mis à jour le 11 décembre 2006 :  
<http://www.sophos.com/support/knowledgebase/article/17609.html>
- Article Sophos concernant les vulnérabilités annoncées par iDefense et Tipping Point, du 08 décembre 2006 :  
<http://www.sophos.com/support/knowledgebase/article/21681.html>
- Référence CVE CVE-2006-6335 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6335>

## Gestion détaillée du document

11 décembre 2006 version initiale.