

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité des antivirus Sophos

---

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-191>

---

### Gestion du document

Référence	CERTA-2006-AVI-191
Titre	Vulnérabilité des antivirus Sophos
Date de la première version	10 mai 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sophos
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

- *Sophos Anti-Virus 3.x, 4.x et 5.x* ;
- *Sophos Anti-Virus Small Business Edition* ;
- *Sophos MailMonitor for Notes/Domino, SMTP* ;
- *Sophos PureMessage for UNIX 4.x, 5.x* ;
- *Sophos PureMessage for Windows/Exchange 2.x* ;
- *Sophos PureMessage Small Business Edition 2.x*.

## 3 Résumé

Un utilisateur mal intentionné peut soumettre à l'antivirus une archive *cab* volontairement construite pour exécuter du code arbitraire.

## 4 Description

Une erreur dans la gestion des tampons mémoire lors de la décompression des archives *cab* peut être exploitée pour exécuter du code arbitraire, si la configuration prévoit l'analyse de telles archives. L'insertion en pièce jointe d'un message vers l'équipement de la victime, permet une action 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 *Sophos* du 08 mai 2006 :  
<http://www.sophos.com/support/knowledgebase/article/4934.html>
- Référence CVE CVE-2006-0994 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0994>

## Gestion détaillée du document

10 mai 2006 version initiale.