

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans l'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-2007-AVI-394>

---

### Gestion du document

Référence	CERTA-2007-AVI-394
Titre	Vulnérabilité dans l'antivirus Sophos
Date de la première version	11 septembre 2007
Date de la dernière version	–
Source(s)	Article Sophos 29146 du 04 septembre 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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

Moteurs d'antivirus *Sophos* antérieurs à la version 2.49.0.

## 3 Résumé

Une vulnérabilité dans le moteur d'antivirus de *Sophos* permet à un utilisateur malintentionné de contourner la politique de sécurité.

## 4 Description

La gestion des fichiers d'archives (CAB, RAR, LZH) avec en-têtes malformés est imparfaite. Une vulnérabilité permet à un utilisateur malveillant de dissimuler au moteur d'antivirus un programme malveillant contenu dans une archive spécialement construite.

## **5 Solution**

La version 2.49.0 du moteur d'antivirus corrige le problème.

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

## **6 Documentation**

- Article de la base de connaissance Sophos 29146 du 04 septembre 2007 :  
<http://sophos.com/support/knowledgebase/article/29146.html>
- Référence CVE CVE-2007-4787 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4787>

## **Gestion détaillée du document**

**11 septembre 2007** version initiale.