

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans les produits 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-2009-AVI-241>

---

### Gestion du document

Référence	CERTA-2009-AVI-241
Titre	Vulnérabilité dans les produits Sophos
Date de la première version	19 juin 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sophos #59992 du 15 juin 2009
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

Systèmes d'exploitation affectés :

- Sophos Email Appliance 3.x ;
- Sophos Web Appliance 2.x.

Applications affectées :

- Sophos Anti-Virus 4.x ;
- Sophos Anti-Virus 6.x ;
- Sophos Anti-Virus 7.x ;
- Sophos PureMessage pour Unix 5.x.

## 3 Résumé

Une vulnérabilité, pouvant conduire à un contournement de la politique de sécurité, a été découverte dans plusieurs produits Sophos.

## **4 Description**

Une vulnérabilité causée par une erreur dans le traitement des archives au format `cab` peut être exploitée par un utilisateur malveillant, au moyen d'une archive au format `cab` spécialement construite afin de contourner la politique de sécurité et outre-passé l'analyse anti-virus.

## **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 #59992 du 15 juin 2009 :  
<http://www.sophos.com/support/knowledgebase/article/59992.html>

## **Gestion détaillée du document**

**19 juin 2009** version initiale.