



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 décembre 2006
N° CERTA-2006-AVI-554

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2006-AVI-554>

Gestion du document

Référence	CERTA-2006-AVI-554
Titre	Vulnérabilité de l'antivirus Sophos
Date de la première version	14 décembre 2006
Date de la dernière version	–
Source(s)	Bulletins de sécurité Sophos du 14 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.

2 Systèmes affectés

- *Sophos antivirus 3.x*;
- *Sophos antivirus 4.x*;
- *Sophos antivirus 5.x*;
- *Sophos antivirus 6.x* pour Windows.

3 Résumé

Deux failles de sécurité de l'antivirus Sophos permettent à un utilisateur malveillant de compromettre à distance le système vulnérable.

4 Description

Une erreur existe dans la bibliothèque `veex.dll` lors du traitement d'archives au format CPIO. Une autre erreur existe dans la même bibliothèque lors du traitement des archives au format SIT (stuffit). Par l'utilisation d'un nom de fichier extrêmement long et non terminé par un caractère `null`, un utilisateur distant peut créer un débordement de mémoire et exécuter du code arbitraire 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 17340 Sophos du 14 décembre 2006 :
<http://www.sophos.com/support/knowledgebase/article/17340.html>
- Bulletin de sécurité 21637 Sophos du 14 décembre 2006 :
<http://www.sophos.com/support/knowledgebase/article/21637.html>
- Référence CVE CVE-2006-6335 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6335>

Gestion détaillée du document

14 décembre 2006 version initiale.