Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 novembre 2006
N° CERTA-2006-AVI-472

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités dans les produits Sophos

Gestion du document

Référence	CERTA-2006-AVI-472
Titre	Plusieurs vulnérabilités dans les produits Sophos
Date de la première version	06 novembre 2006
Date de la dernière version	–
Source(s)	Article de Sophos du 02 novembre 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

- Déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Sophos Anti-Virus 6.X, pour la version 6.0.5 ainsi que celles antérieures ;
- Sophos Anti-Virus 4.X, pour la version 4.11, ainsi que celles antérieures ;
- Sophos Anti-Virus Mac OS X, pour la version 4.8.5, ainsi que celles antérieures ;
- Sophos Endpoint Security, pour la version 6.0.5 ainsi que celles antérieures.

3 Description

Plusieurs vulnérabilités ont été identifiées dans les produits Sophos, dont Sophos Anti-Virus. Parmi celles-ci, l'une affecterait le module `Petite`, qui gère les fichiers compressés par l'application du même nom. D'autres seraient dues à une mauvaise manipulation de documents au format `RAR` ou `CHM` (fichiers d'aide Microsoft).

Une personne malveillante pourrait construire un document exploitant l'une de ces vulnérabilités, afin de perturber le système possédant une version de Sophos vulnérable, et empêchant ainsi le service de fonctionner correctement.

4 Solution

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

5 Documentation

- Article Sophos du 0é novembre 2006, issu de la Base de Connaissances :
  http://www.sophos.fr/support/knowledgebase/article/7618.html
- Bulletin de sécurité iDefense du 31 octobre 2006 :
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=438
- Référence CVE CVE-2006-4839 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4839

Gestion détaillée du document

06 novembre 2006 version initiale.