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 septembre 2006
N° CERTA-2006-AVI-394

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de l'antivirus Symantec

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-394

Gestion du document

Référence	CERTA-2006-AVI-394
Titre	Multiples vulnérabilités de l'antivirus Symantec
Date de la première version	14 septembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec du 13 septembre 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 ;
- exécution de commandes arbitraires à distance ;
- élévation de privilèges.

2 Systèmes affectés

- Symantec AntiVirus Corporate Edition 10.0 ;
- Symantec AntiVirus Corporate Edition 9.x ;
- Symantec AntiVirus Corporate Edition 8.1 ;
- Symantec Client Security 3.0 ;
- Symantec Client Security 2.x ;
- Symantec Client Security 1.x.

3 Résumé

Deux vulnérabilités permettant respectivement d'exécuter du code arbitraire à distance ou de provoquer un déni de service ont été découverte dans le logiciel antivirus de Symantec.

4 Description

Deux vulnérabilités ont été découvertes dans les suites logicielles antivirus de Symantec :

- la première vulnérabilité résulte d'une erreur dans le traitement d'un message de notification malformé. Un utilisateur mal intentionné peut, grâce à un message spécialement construit, exécuter des commandes arbitraires à distance. Ces commandes sont exécutées avec les privilèges `SYSTEM` ;
- la seconde vulnérabilité est présente au niveau du module de vérification en temps réel. Cette vulnérabilité peut être exploitée par l'intermédiaire d'un message de notification spécialement construit, conduisant alors à un déni de service.

5 Solution

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

6 Documentation

- Site de l'éditeur :
  http://www.symantec.com
- Bulletin de sécurité de l'éditeur du 13 septembre 2006 :
  http://securityresponse.symantec.com/avcenter/security/Content/2006.09.13.html
- Référence CVE CVE-2006-3454 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3454

Gestion détaillée du document

14 septembre 2006 version initiale.