Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juin 2006
N° CERTA-2006-AVI-221-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Symantec AntiVirus et Client Security

Gestion du document

Référence	CERTA-2006-AVI-221-001
Titre	Vulnérabilité dans Symantec AntiVirus et Client Security
Date de la première version	28 mai 2006
Date de la dernière version	13 juin 2006
Source(s)	Bulletin de sécurité Symantec du 27 mai 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 ;
- déni de service à distance.

2 Systèmes affectés

- La version 10.0 de Symantec AntiVirus Corporate Edition pour Microsoft Windows ;
- la version 10.1 de Symantec AntiVirus Corporate Edition pour Microsoft Windows ;
- la version 3.0 de Symantec Security Client pour Microsoft Windows ;
- la version 3.1 de Symantec Security Client pour Microsoft Windows.

Les produits vendus sous la marque Norton ne sont pas affectés.

3 Résumé

Une vulnérabilité a été identifiée dans certaines versions des produits Symantec AntiVirus Corporate Edition et Symantec Client Security. Un utilisateur malveillant distant peut profiter de celle-ci pour perturber le système hébergeant le service Symantec ou y exécuter des commandes arbitraires.

4 Description

Une vulnérabilité de type débordement de pile (ou `stack overflow`) a été identifiée dans certaines versions des produits Symantec AntiVirus Corporate Edition et Symantec Client Security. Une pile est une structure logique destinée à contenir des données. Cette vulnérabilité se situe au niveau de la console de gestion distante, qui est généralement activée en écoute par défaut sur le port TCP 2967. Elle ne vérifie pas correctement les données de certaines requêtes envoyées à `Rtvscan.exe`. Un utilisateur malveillant distant peut profiter de cette vulnérabilité pour perturber le système hébergeant le service Symantec ou y exécuter des commandes arbitraires.

5 Solution

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

6 Documentation

- Bulletin de sécurité Symantec SYM06-010, mis à jour le 27 mai 2006 :
  http://www.symantec.com/avcenter/security/Content/2006.05.25.html
- Correctifs Symantec disponibles à l'adresse suivante :
  http://www.symantec.com/techsupp/enterprise/
- Bulletin de sécurité eEye AD20060612 du 12 juin 2006 :
  http://www.eeye.com/html/research/advisories/AD20060612.html
- Référence CVE CVE-2006-2630 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2630

Gestion détaillée du document

28 mai 2006 version initiale.
12 juin 2006 ajout référence CVE et bulletin eEye.