

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans certains produits 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-463>

Gestion du document

Référence	CERTA-2006-AVI-463
Titre	Vulnérabilité dans certains produits Symantec
Date de la première version	25 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM06-022 du 23 octobre 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 ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- Symantec AntiVirus Corporate Edition 8.1 ;
- Symantec AntiVirus Corporate Edition pour la version 9.0.3 ainsi que celles antérieures ;
- Symantec Client Security version 1.1 ;
- Symantec Client Security pour la version 2.0.3 ainsi que celles antérieures.

3 Résumé

Une vulnérabilité a été identifiée dans certains produits de sécurité Symantec. Une personne malveillante locale au système pourrait exploiter celle-ci pour élever ses droits à ceux de l'administrateur, voire exécuter des commandes arbitraires sur la machine ayant une version vulnérable.

4 Description

Une vulnérabilité a été identifiée dans certains produits de sécurité Symantec. Elle provient d'un pilote particulier, `SAVRT.SYS`, installé par défaut.

Une application particulière dans les produits communique avec les pilotes : `DeviceIOControl`. Le pilote ne vérifierait pas correctement un espace d'adressage au cours de la communication avec cette dernière.

La vulnérabilité pourrait donc être exploitée par une personne locale au système, qui enverrait des données spécifiques via la fonction `DeviceIOControl()`. Cela lui permettrait d'élever ses droits à ceux de l'administrateur, voire exécuter des commandes arbitraires sur la machine ayant une version vulnérable.

5 Solution

Se référer au bulletin de sécurité SYM06-022 de l'éditeur Symantec pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Référence CVE CVE-2006-3455 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3455>
- Bulletin de sécurité Symantec SYM06-022 du 23 octobre 2006 :
<http://www.symantec.com/avcenter/security/Content/2006.10.23.html>

Gestion détaillée du document

25 octobre 2006 version initiale.