



Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Symantec Scan Engine

---

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-169>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2006-AVI-169                                       |
| Titre                       | Vulnérabilités dans Symantec Scan Engine                 |
| Date de la première version | 24 avril 2006  |
| Date de la dernière version | –  |
| Source(s)                   | Bulletin de sécurité Symantec SYM06-008 du 21 avril 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

- Accès non autorisé ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

*Symantec Scan Engine* version 5.0.

## 3 Description

Trois vulnérabilités ont été découvertes dans *Symantec Scan Engine* :

- *Symantec Scan Engine* n'authentifie pas correctement les utilisateurs qui se connectent par l'interface d'administration. Un utilisateur mal intentionné peut obtenir les droits de l'administrateur de *Symantec Scan Engine* en utilisant l'interface d'administration ;
- *Symantec Scan Engine* utilise une clé privée statique DSA pour ses communications en SSL. Cette clé ne peut pas être modifiée par les utilisateurs mais peut être facilement exportée. Un utilisateur mal intentionné peut récupérer cette clé pour réaliser des attaques de type *man-in-the-middle* ;
- une vulnérabilité permet de télécharger sans authentification préalable les fichiers situés dans le répertoire d'installation de *Symantec Scan Engine*.

## **4 Contournement provisoire**

Filtrer les ports 8004/tcp et 8005/tcp.

## **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 SYM06-008 du 21 avril 2006 :  
<http://www.symantec.com/avcenter/security/Content/2006.04.21.html>

## **Gestion détaillée du document**

**24 avril 2006** version initiale.