Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 juin 2004
N° CERTA-2004-AVI-193-001

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

**Objet : Vulnérabilité du logiciel OfficeScan de Trend Micro**

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-2004-AVI-193`

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2004-AVI-193-001 |
| Titre | Vulnérabilité du logiciel OfficeScan de Trend Micro |
| Date de la première version | 11 juin 2004 |
| Date de la dernière version | 22 juin 2004 |
| Source(s) | Bulletin de Trend Micro |
| 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

Elévation de privilèges.

## 2 Systèmes affectés

Trend Micro OfficeScan Corporate Edition 5.X.

## 3 Description

Lors de la détection d'un virus par le logiciel OfficeScan, une fenêtre est ouverte par le service `ntrtscan.exe` avec les privilèges de ce dernier (SYSTEM par défaut).

Via l'application d'aide en ligne accessible depuis cette fenêtre, il est alors possible pour un utilisateur mal intentionné de lancer des applications avec les privilèges du service `ntrtscan.exe`.

## 4 Solution

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

# 5 Documentation

- OfficeScan Corporate Edition 5.58 Hot Fix - Build 1089 :
  http://uk.trendmicro-europe.com/enterprise/support/knowledge_base_detail.php?solutionId=20118
- Message "Trend OfficeScan local privilege escalation" dans la liste de diffusion full-disclosure :
  http://marc.theaimsgroup.com/?l=full-disclosure&m=108681850225356&w=2

# Gestion détaillée du document

**11 juin 2004** version initiale.
**22 juin 2004** mise-à-jour de la section Systèmes affectés.