

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilité du produit Trend Micro Office Scan

---

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-533>

---

### Gestion du document

Référence	CERTA-2006-AVI-533
Titre	Multiples vulnérabilité du produit Trend Micro Office Scan
Date de la première version	06 décembre 2006
Date de la dernière version	–
Source(s)	Bulletin de mise à jour 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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

- Trend Micro OfficeScan version 6.5 et versions antérieures ;
- Trend Micro OfficeScan version 7.3 et versions antérieures.

## 3 Résumé

Plusieurs vulnérabilités ont été découvertes dans le produit Trend Micro OfficeScan.

## 4 Description

Deux vulnérabilités ont été découvertes dans le produit Trend Micro OfficeScan. Ces vulnérabilités résultent d'une mauvaise gestion de la mémoire par les modules Wizard.exe et CgiRemoteInstall.exe. Ces erreurs peuvent être exploitées par un utilisateur malintentionné afin d'exécuter du code arbitraire à distance.

L'attaquant doit cependant être authentifié afin d'exploiter cette vulnérabilité.

## 5 Solution

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

## 6 Documentation

- Bulletin de mise à jour de Trend Micro pour OfficeScan 6.5 et 7.3 :  
[http://www.trendmicro.com/ftp/products/patches/OSCE\\_6.5\\_win\\_en\\_patch8.exe](http://www.trendmicro.com/ftp/products/patches/OSCE_6.5_win_en_patch8.exe)  
[http://www.trendmicro.com/ftp/products/patches/osce\\_73\\_win\\_en\\_patch1.1.exe](http://www.trendmicro.com/ftp/products/patches/osce_73_win_en_patch1.1.exe)
- Référence CVE CVE-2006-6179 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6179>
- Référence CVE CVE-2006-6180 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6180>

## Gestion détaillée du document

**06 décembre 2006** version initiale.