

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Trend Micro OfficeScan

---

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-2007-AVI-279>

---

### Gestion du document

Référence	CERTA-2007-AVI-279
Titre	Vulnérabilités dans Trend Micro OfficeScan
Date de la première version	27 juin 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Trend Micro du 26 juin 2007
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

*Trend Micro OfficeScan Corporate Edition* version 8.0.

## 3 Résumé

Deux vulnérabilités dans *Trend Micro OfficeScan* permettent l'exécution de code arbitraire à distance et un contournement de la politique de sécurité.

## 4 Description

Deux vulnérabilités ont été découvertes dans les modules CGI du serveur *Trend Micro OfficeScan* :

- la première, de type débordement de mémoire, permet l'exécution de code arbitraire à distance avec les droits de l'utilisateur web ;

- la seconde permet, par l'intermédiaire de paquets HTTP dont les en-têtes ont été spécifiquement modifiés, de se connecter à la console d'administration en contournant le mécanisme d'authentification.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Trend Micro du 26 juin 2007 :  
[http://www.trendmicro.com/ftp/documentation/readme/osce\\_80\\_win\\_en\\_securitypatch\\_b1042\\_readme.txt](http://www.trendmicro.com/ftp/documentation/readme/osce_80_win_en_securitypatch_b1042_readme.txt)

## **Gestion détaillée du document**

**27 juin 2007** version initiale.