



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 15 mars 2007  
N° CERTA-2007-AVI-127

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans les produits 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-2007-AVI-127>

---

### Gestion du document

Référence	CERTA-2007-AVI-127
Titre	Vulnérabilité dans les produits Trend Micro
Date de la première version	15 mars 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDefense 488 du 14 mars 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

- Déni de service à distance ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

Les outils de Trend Micro dont le moteur de balayage (*Scan Engine*) a une version antérieure ou égale à 8.300 ou 8.000.

## 3 Description

Une vulnérabilité a été identifiée dans plusieurs produits de sécurité Trend Micro. Elle provient du pilote *VsapiNT.sys*, qui surveille différents formats de fichiers à la recherche de contenus malveillants. Les fichiers exécutables, compressés au format UPX (pour the Ultimate Packer for eXecutables), ne seraient pas correctement manipulés.

Une personne malveillante pourrait profiter de cette vulnérabilité pour construire un fichier particulier. Quand celui-ci sera contrôlé par le système vulnérable, à la réception d'un courrier électronique ou au cours d'un téléchargement par exemple, il risque de perturber le noyau et provoquer une erreur de type 'écran bleu' (ou *Blue Screen of Death*).

## **4 Solution**

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

## **5 Documentation**

- Bulletin de sécurité iDefense du 14 mars 2007 :  
<http://www.idefense.com/application/poi/display?id=488>
- Annonce de sécurité Trend Micro du 14 mars 2007 :  
<http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034587>

## **Gestion détaillée du document**

**15 mars 2007** version initiale.