

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des 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-073>

Gestion du document

Référence	CERTA-2007-AVI-073
Titre	Vulnérabilités des produits Trend Micro
Date de la première version	08 février 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité Trend Micro du 07 février 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 ;
- élévation de privilèges ;
- déni de service à distance.

2 Systèmes affectés

- Trend Micro PC-cillin Internet Security 2007 ;
- Trend Micro Antivirus 2007 ;
- Trend Micro Anti-Spyware (SMB 3.2 SP1, Consumer 3.5, Enterprise 3.0 SP2) ;
- Client / Server / Messaging Security pour SMB 3.5 ;
- Damage Cleanup Services 3.2.

3 Résumé

Deux vulnérabilités ont été identifiées dans certains produits Trend Micro. Elles permettraient à une personne malveillante qui les exploiterait, d'élever ses privilèges, de lancer un déni de service ou d'exécuter des commandes arbitraire à distance sur le système vulnérable.

4 Description

Deux vulnérabilités ont été identifiées dans certains produits Trend Micro.

1. les fichiers exécutables compressés par UPX ne seraient pas correctement manipulés par les produits de Trend Micro. Il serait possible d'en construire un de manière particulière, afin de provoquer un débordement de la pile. Cela provoquerait une perturbation du système de balayage de fichiers, voire, éventuellement, une exécution de code arbitraire.
2. le fichier (pilote) TmComm.sys ne s'installerait pas avec des droits nécessaires et suffisants. Il offrirait un droit d'écriture pour tous. Une personne malveillante pourrait exploiter cette vulnérabilité afin d'élever ses privilèges sur le système vulnérable.

5 Solution

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

6 Documentation

- Avis de sécurité IDefense Labs 470 du 07 février 2007 :
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=470>
- Avis de sécurité IDefense Labs 469 du 07 février 2007 :
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=469>
- Bulletin de sécurité Trend Micro 1034289 du 06 février 2007 :
<http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034289>
- Bulletin de sécurité Trend Micro 1034432 du 07 février 2007 :
<http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034432>

Gestion détaillée du document

08 février 2007 version initiale.