

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Trend Micro OfficeScan Server

---

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-2008-AVI-459>

---

### Gestion du document

Référence	CERTA-2008-AVI-459
Titre	Vulnérabilité dans Trend Micro OfficeScan Server
Date de la première version	15 septembre 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité Trend Micro du 12 septembre 2008
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 Client Server Messaging Security for SMB 2.x ;
- Trend Micro Client Server Messaging Security for SMB 3.x ;
- Trend Micro OfficeScan Corporate Edition 7.x ;
- Trend Micro OfficeScan Corporate Edition 8.x.

## 3 Résumé

Une vulnérabilité dans les produits Trend Micro permet à un utilisateur distant malintentionné d'exécuter du code arbitraire à distance.

## 4 Description

Une vulnérabilité de type de débordement de mémoire a été découverte dans l'application `cgiRecvFile.exe`. Cette vulnérabilité peut être exploitée au moyen d'une requête HTTP spécialement construite afin d'exécuter du code arbitraire à distance.

## 5 Solution

Les correctifs de sécurité sont disponibles sur le site de l'éditeur aux adresses suivantes :

[http://www.trendmicro.com/ftp/products/patches/CSM\\_3.6\\_OSCE\\_7.6\\_Win\\_EN\\_CriticalPatch\\_B1195.exe](http://www.trendmicro.com/ftp/products/patches/CSM_3.6_OSCE_7.6_Win_EN_CriticalPatch_B1195.exe)

[http://www.trendmicro.com/ftp/products/patches/OSCE\\_7.3\\_Win\\_EN\\_CriticalPatch\\_B1367.exe](http://www.trendmicro.com/ftp/products/patches/OSCE_7.3_Win_EN_CriticalPatch_B1367.exe)

[http://www.trendmicro.com/ftp/products/patches/OSCE\\_8.0\\_SP1\\_Patch1\\_Win\\_EN\\_CriticalPatch\\_B3060.exe](http://www.trendmicro.com/ftp/products/patches/OSCE_8.0_SP1_Patch1_Win_EN_CriticalPatch_B3060.exe)

[http://www.trendmicro.com/ftp/products/patches/OSCE\\_8.0\\_SP1\\_Win\\_EN\\_CriticalPatch\\_B2424.exe](http://www.trendmicro.com/ftp/products/patches/OSCE_8.0_SP1_Win_EN_CriticalPatch_B2424.exe)

[http://www.trendmicro.com/ftp/products/patches/OSCE\\_8.0\\_Win\\_EN\\_CriticalPatch\\_B1361.exe](http://www.trendmicro.com/ftp/products/patches/OSCE_8.0_Win_EN_CriticalPatch_B1361.exe)

## 6 Documentation

– Bulletins de sécurité Trend Micro du 12 septembre 2008 :

[http://www.trendmicro.com/ftp/documentation/readme/CSM\\_3.6\\_OSCE\\_7.6\\_Win\\_EN\\_CriticalPatch\\_B1195\\_readme.txt](http://www.trendmicro.com/ftp/documentation/readme/CSM_3.6_OSCE_7.6_Win_EN_CriticalPatch_B1195_readme.txt)

[http://www.trendmicro.com/ftp/documentation/readme/OSCE\\_7.3\\_Win\\_EN\\_CriticalPatch\\_B1367\\_readme.txt](http://www.trendmicro.com/ftp/documentation/readme/OSCE_7.3_Win_EN_CriticalPatch_B1367_readme.txt)

[http://www.trendmicro.com/ftp/documentation/readme/OSCE\\_8.0\\_SP1\\_Patch1\\_Win\\_EN\\_CriticalPatch\\_B3060\\_readme.txt](http://www.trendmicro.com/ftp/documentation/readme/OSCE_8.0_SP1_Patch1_Win_EN_CriticalPatch_B3060_readme.txt)

[http://www.trendmicro.com/ftp/documentation/readme/OSCE\\_8.0\\_SP1\\_Win\\_EN\\_CriticalPatch\\_B2424\\_readme.txt](http://www.trendmicro.com/ftp/documentation/readme/OSCE_8.0_SP1_Win_EN_CriticalPatch_B2424_readme.txt)

[http://www.trendmicro.com/ftp/documentation/readme/OSCE\\_8.0\\_Win\\_EN\\_CriticalPatch\\_B1361\\_readme.txt](http://www.trendmicro.com/ftp/documentation/readme/OSCE_8.0_Win_EN_CriticalPatch_B1361_readme.txt)

– Référence CVE CVE-2008-2437 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2437>

## Gestion détaillée du document

15 septembre 2008 version initiale.