

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans divers 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-2008-AVI-427>

Gestion du document

Référence	CERTA-2008-AVI-427
Titre	Vulnérabilité dans divers produits Trend Micro
Date de la première version	22 août 2008
Date de la dernière version	–
Source(s)	Correctif de sécurité Trend Micro OfficeScan 8.0 SP1 du 22 août 2008 Correctif de sécurité Trend Micro Worry-Free Business Security 5.0 du 20 août 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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Trend Micro Client Server Messaging Security for SMB versions 3.x ;
- Trend Micro OfficeScan Corporate Edition versions 7.x ;
- Trend Micro OfficeScan Corporate Edition versions 8.x ;
- Trend Micro Worry-Free Business Security versions 5.x.

3 Résumé

Une vulnérabilité dans divers produits *Trend Micro* permet de contourner la phase d'authentification.

4 Description

Une vulnérabilité a été découverte dans divers produits *Trend Micro*. Un utilisateur malintentionné peut obtenir le contrôle de la console Web lorsqu'un administrateur *OfficeScan* se connecte.

5 Solution

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

6 Documentation

- Correctif de sécurité Trend Micro OfficeScan 8.0 SP1 du 22 août 2008 :
http://www.trendmicro.com/ftp/documentation/readme/OSCE_8.0_SP1_Win_EN_CriticalPatch_B2402_readme.txt
- Correctif de sécurité Trend Micro Worry-Free Business Security 5.0 du 20 août 2008 :
http://www.http://www.trendmicro.com/ftp/documentation/readme/Readme_WFBS5%200_EN_CriticalPatch1404.txt
- Référence CVE CVE-2008-2433 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2433>

Gestion détaillée du document

22 août 2008 version initiale.