

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2009-AVI-026>

Gestion du document

Référence	CERTA-2009-AVI-026
Titre	Multiples vulnérabilités dans Trend Micro OfficeScan
Date de la première version	21 janvier 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Trend Micro du 16 janvier 2009
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 ;
- contournement de la politique de sécurité ;
- déni de service.

2 Systèmes affectés

Trend Micro OfficeScan version 8.x.

3 Résumé

Plusieurs vulnérabilités affectant Trend Micro OfficeScan permettent à une personne malintentionnée d'effectuer un déni de service, d'exécuter du code arbitraire ou de contourner la politique de sécurité.

4 Description

De multiples vulnérabilités ont été découvertes dans Trend Micro OfficeScan :

- des erreurs dans la validation des entrées dans le service OfficeScan NT Firewall permettent d'exécuter du code arbitraire avec les droits *SYSTEM* ou de provoquer un déni de service ;
- une manipulation de la configuration est possible pour un utilisateur local via des paquets spécialement conçus malgré la restriction par mot de passe activée pour manipuler l'interface de configuration.

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 16 janvier 2009 :
http://www.trendmicro.com/ftp/documentation/readme/OSCE8.0_SP1_Patch1_CriticalPatch_3191_Readme.txt
- Référence CVE CVE-2008-3864 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3864>
- Référence CVE CVE-2008-3865 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3865>
- Référence CVE CVE-2008-3866 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3866>

Gestion détaillée du document

21 janvier 2009 version initiale.