

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-2005-AVI-089>

Gestion du document

Référence	CERTA-2005-AVI-089
Titre	Vulnérabilité dans les produits Trend Micro
Date de la première version	28 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Trend Micro du 23 février 2005
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 Suite for SMB for Windows ;
- Trend Micro Client / Server Suite for SMB for Windows ;
- Trend Micro InterScan eManager ;
- Trend Micro InterScan Messaging Security Suite for Linux ;
- Trend Micro InterScan Messaging Security Suite for Windows ;
- Trend Micro InterScan Viruswall for AIX ;
- Trend Micro InterScan Viruswall for HP-UX ;
- Trend Micro InterScan Viruswall for Linux ;
- Trend Micro InterScan Viruswall for SMB ;
- Trend Micro InterScan Viruswall for Solaris ;
- Trend Micro InterScan Viruswall for Windows ;
- Trend Micro InterScan Web Security Suite for Linux ;
- Trend Micro InterScan Web Security Suite for Solaris ;

- Trend Micro InterScan Web Security Suite for Windows ;
- Trend Micro InterScan WebManager ;
- Trend Micro InterScan WebProtect for ISA ;
- Trend Micro OfficeScan Corp. Edition ;
- Trend Micro PC-cillin Internet Security ;
- Trend Micro PortalProtect for Sharepoint ;
- Trend Micro ScanMail eManager ;
- Trend Micro ScanMail for Lotus Domino on AIX ;
- Trend Micro ScanMail for Lotus Domino on AS/400 ;
- Trend Micro ScanMail for Lotus Domino on S/390 ;
- Trend Micro ScanMail for Lotus Domino on Solaris ;
- Trend Micro ScanMail for Lotus Domino on Windows ;
- Trend Micro for Microsoft Exchange ;
- Trend Micro ServerProtect for Linux ;
- Trend Micro ServerProtect for Windows.

3 Résumé

Une vulnérabilité dans le traitement des archives ARJ par les produits Trend Micro permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité a été découverte dans le traitement des fichiers archive au format ARJ par le moteur VSAPI des produits Trend Micro.

Un utilisateur mal intentionné peut, par le biais d'un fichier ARJ malicieusement constitué, exécuter du code arbitraire à distance.

5 Solution

Mettre à jour le moteur VSAPI en version 7.510 ou ultérieure (cf Documentation).

6 Documentation

- Bulletin de sécurité Trend Micro du 23 février 2005 :
<http://www.trendmicro.com/vinfo/secadvisories/default6.asp?VName=Vulnerability+in+VSAPI+ARJ+parsing+could+allow+>
- Mise à jour du moteur VSAPI :
<http://www.trendmicro.com/download/engine.asp>

Gestion détaillée du document

28 février 2005 version initiale.