Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 24 septembre 2001
N° CERTA-2001-AVI-098

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le logiciel Interscan eManager de 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-2001-AVI-098

Gestion du document

Référence	CERTA-2001-AVI-098
Titre	Vulnérabilités dans le logiciel Interscan eManager de Trend Micro
Date de la première version	24 septembre 2001
Date de la dernière version	–
Source(s)	Cert-IST Trend Micro
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

- déni de service sur le serveur IIS ;
- exécution distante de code arbitraire avec des privilèges locaux ;
- reconfiguration du filtrage à l'insu de l'administrateur.

2 Systèmes affectés

Trend Micro Interscan eManager pour NT ;

3 Description

Le logiciel Interscan de Trend Micro est un logiciel de filtrage de certains protocoles courants destiné aux passerelles Internet. Le module eManager est un greffon optionnel au logiciel Interscan. Ce greffon est spécialisé dans le filtrage des méls.

eManager permet la configuration du filtrage par le WEB. Des scripts CGI qui permettent cette configuration sont vulnérables au débordement de variable. Ces vulnérabilités permettent à n'importe quel individu mal intentionné d'exécuter à distance du code avec les droits associés au contexte local, dans la mesure où il n'y aucune authentification.

4 Contournement provisoire

- Supprimer le répertoire virtuel `/eManager` à l'aide de `Internet Service Manager` si la console d'administration par le WEB n'est pas nécessaire ;
- Mettre en place une authentification par Windows (NTLM) afin de restreindre l'accès à la console d'administration par le WEB ;
- Interdire, au niveau du pare-feu, les accès à la console d'administration par le WEB aux sites auxquels on ne fait pas confiance.

5 Solution

Appliquer le correctif fourni par Trend Micro :
ftp://ftp.trendmicro.fr/pub/trendmicro/produitsfull/isnt/patchs/ISEM352_HotFix_1521.zip

6 Documentation

Gestion détaillée du document

24 septembre 2001 version initiale.