



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 septembre 2002
N° CERTA-2002-AVI-216

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des anti-virus pour passerelles de messagerie

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-2002-AVI-216>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2002-AVI-216 |
| Titre | Vulnérabilité des anti-virus pour passerelles de messagerie |
| Date de la première version | 20 septembre 2002 |
| Date de la dernière version | – |
| Source(s) | SecurityFocus |
| 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 des mécanismes de protection des anti-virus pour passerelles de messagerie.

2 Systèmes affectés

- InterScan VirusWall Trend Micro versions antérieures à la 3.52 ;
- MailSweeper Clearswift ;
- Mimedefang Roaring Penguin versions antérieures à la 2.21.

3 Résumé

Un utilisateur mal intentionné peut contourner la protection offerte par les anti-virus pour passerelles de messagerie en fragmentant, lors de l'envoi, des fichiers à risque.

4 Description

Différents logiciels de messagerie sont compatibles avec la RFC 2046 qui permet d'envoyer des messages volumineux en les fragmentant.

Cette fragmentation est transparente pour l'utilisateur, le message étant automatiquement reconstitué par le client de messagerie.

Plusieurs scanners de messagerie analysent les messages fragmentés sans les reconstituer et sont donc susceptibles de ne pas intercepter les messages ayant une charge virale.

5 Solution

- Télécharger InterScan VirusWall Trend Micro 3.52 pour Microsoft Windows :
ftp://ftp-download.trendmicro.com.ph/Gateway/ISNT/3.52/Hotfix_build1494_v352_Smtp_case6593.zip
- MailSweeper Clearswif :
Mettre en place une analyse lexicale du champ Content-Type (pour plus de détails se référer au bulletin du constructeur, Cf Section Documentation)
- Mimedefang Roaring Penguin :
Appliquer la version 2.21 (Cf Section Documentation)

6 Documentation

- InterScan VirusWall Trend Micro :
<http://securityresponse.symantec.com/avcenter/security/Content/2002.09.10.html>
- MailSweeper Clearswif :
<http://www.mimesweeper.com/support/threatlab/message.asp>
- Mimedefang Roaring Penguin :
<http://www.roarinpenguin.com/mimedefang>

Gestion détaillée du document

20 septembre 2002 version initiale.