Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 janvier 2006
N° CERTA-2006-AVI-035

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités des logiciels antivirus F-Secure

Gestion du document

Référence	CERTA-2006-AVI-035
Titre	Multiples vulnérabilités des logiciels antivirus F-Secure
Date de la première version	19 janvier 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité F-Secure numéro FSC-2006-1
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- F-Secure Anti-virus 2004, 2005 et 2006;
- F-Secure Anti-virus 5.x;
- F-Secure Anti-virus Client Security 5.x;
- F-Secure Anti-virus Client Security 6.x;
- F-Secure Anti-virus for Citrix Servers 5.x;
- F-Secure Anti-virus for Firewalls 6.x;
- F-Secure Anti-virus for Linux 4.x;
- F-Secure Anti-virus for Microsoft Exchange 6.x;
- F-Secure Anti-virus for MIMEsweeper 5.x;
- F-Secure Anti-virus for Samba Servers 5.x;
- F-Secure Anti-virus for Windows Servers 5.x;
- F-Secure Anti-virus for Workstations 5.x;

- F-Secure Internet Gatekeeper 6.x ;
- F-Secure Internet Gatekeeper for linux 2.x ;
- F-Secure Internet Security 2004, 2005 et 2006 ;
- F-Secure Personal Expresse.

3 Résumé

Deux vulnérabilités ont été découvertes dans plusieurs produits F-Secure. Ces vulnérabilités peuvent conduire au contournement de la politique anti-virale et/ou à l'exécution de code arbitraire à distance.

4 Description

Deux vulnérabilités ont été découvertes dans plusieurs produit F-Secure :

- La première consiste en une mauvaise gestion des archives `ZIP`. Cette vulnérabilité peut être exploitée via une archive `ZIP` malicieusement construite, et ainsi provoquer un débordement de mémoire permettant l'exécution de code arbitraire ;
- La seconde consiste en une mauvaise gestion des archives ZIP et RAR. Cette vulnérabilité peut être exploitée afin de passer outre la détection de logiciel malveillant.

5 Solution

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

6 Documentation

- Bulletin de sécurité de F-Secure FSC-2006-1 :
  http://www.f-secure.com/security/fsc-2006-1.shtml

Gestion détaillée du document

19 janvier 2006 version initiale.