

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits F-Secure

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-177>

Gestion du document

Référence	CERTA-2009-AVI-177
Titre	Vulnérabilité dans les produits F-Secure
Date de la première version	11 mai 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité F-Secure FSC-2009-1 du 06 mai 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

Contournement de la politique de sécurité.

2 Systèmes affectés

- F-Secure Antivirus for Microsoft Exchange jusqu'à la version 7.10 ;
- F-Secure Internet Gatekeeper :
 - for Windows jusqu'à la version 6.61 ;
 - for Linux jusqu'à la version 2.16 ;
 - for Linux Japanese jusqu'à la version 3.01 ;
- F-Secure Protection Service for Business - E-mail and Server security, jusqu'à la version 8.00 ;
- F-Secure Protection Service for Business - Workstation security, jusqu'à la version 8.00 ;
- F-Secure Protection Service for Consumers, jusqu'à la version 8.00 ;
- F-Secure Internet Security jusqu'à la version 2009 ;
- F-Secure Anti-Virus jusqu'à la version 2009 ;
- F-Secure Home Server Security jusqu'à la version 2009 ;
- F-Secure Client Security jusqu'à la version 8.0 ;
- F-Secure Anti-Virus for Workstations jusqu'à la version 8.0 ;

- F-Secure Anti-Virus for Windows Servers jusqu’à la version 8.00 ;
- F-Secure Anti-Virus for Citrix Servers jusqu’à la version 7.00 ;
- F-Secure Anti-Virus for MIMESweeper jusqu’à la version 5.61 ;
- F-Secure Anti-Virus Linux Client Security jusqu’à la version 5.54 ;
- F-Secure Anti-Virus Linux Server Security jusqu’à la version 5.54 ;
- F-Secure Anti-Virus Linux Servers jusqu’à la version 4.65 ;
- F-Secure Linux Security jusqu’à la version 7.02.

3 Résumé

Un défaut dans l’analyse de formats d’archives permet à un utilisateur malveillant de contourner la politique de sécurité.

4 Description

Un défaut dans l’analyse des fichiers d’archives aux formats *ZIP* et *RAR* permet à un utilisateur malveillant de faire échapper un code malveillant à l’analyse antivirale.

5 Solution

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

6 Documentation

- Bulletin de sécurité F-Secure FSC-2009-1 du 06 mai 2009 :
http://www.f-secure.com/en_EMEA/support/security-advisory/fsc-2009-1.html

Gestion détaillée du document

11 mai 2009 version initiale.