

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2010-AVI-166>

Gestion du document

Référence	CERTA-2010-AVI-166
Titre	Vulnérabilité dans F-Secure
Date de la première version	13 avril 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité F-Secure FSC-2010-1 du 12 avril 2010
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 Anti-Virus pour Microsoft Exchange 9 et antérieures ;
- F-Secure Internet Gatekeeper pour Windows 6.61 et antérieures ;
- F-Secure Internet Gatekeeper pour Linux 4.02 et antérieures ;
- F-Secure Anti-Virus pour MIMESweeper 5.61 et antérieures ;
- F-Secure Anti-Virus 2010 et antérieures ;
- F-Secure Home Server Security 2009 ;
- Solutions basées sur F-Secure Protection Service pour Consumers version 9 et antérieures ;
- Solutions basées sur F-Secure Protection Service pour Business - Workstation security version 9 et antérieures ;
- Solutions basées sur F-Secure Protection Service pour Business - Server Security version 8 et antérieures ;
- Services basés sur F-Secure Mac Protection build 8060 et antérieures ;
- F-Secure Client Security 9 et antérieures ;
- F-Secure Anti-Virus pour Workstations 9 et antérieures ;

- F-Secure Anti-Virus pour Windows Servers 9 et antérieures ;
- F-Secure Linux Security 7.03 et antérieures ;
- F-Secure Anti-Virus Linux Client Security 5.54 et antérieures ;
- F-Secure Anti-Virus Linux Server Security 5.54 et antérieures ;
- F-Secure Anti-Virus pour Linux Servers 4.65 ;
- F-Secure Anti-Virus pour Citrix Servers 9 et antérieures.

3 Résumé

Une vulnérabilité dans la gestion des archives *7Z*, *GZIP*, *CAB* ou *RAR* permet de contourner le moteur de détection de l'*Anti-Virus*.

4 Description

Une vulnérabilité dans les produits F-Secure permet, à une personne malveillante, de construire des archives (*7Z*, *GZIP*, *CAB* ou *RAR*) spécialement formées contournant le moteur de détection de l'*Anti-Virus*. Les fichiers malveillants contenus dans ces archives ne seront donc pas détectés.

Cependant cela n'affecte pas le mécanisme de détection lorsque ces fichiers sont extraits des archives.

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-2010-1 du 12 avril 2010 :
http://www.f-secure.com/en_EMEA/support/security-advisory/fsc-2010-1.html

Gestion détaillée du document

13 avril 2010 version initiale.