Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 février 2005
N° CERTA-2005-AVI-065-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits F-Secure

Gestion du document

Référence	CERTA-2005-AVI-065-001
Titre	Vulnérabilité dans les produits F-Secure
Date de la première version	11 février 2005
Date de la dernière version	14 février 2005
Source(s)	Bulletin de sécurité F-Secure FSC-2005-1 du 10 février 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire.

2 Systèmes affectés

- F-Secure Anti-Virus for Workstation version 5.43 et versions précédentes ;
- F-Secure Anti-Virus for Windows Servers version 5.50 et versions précédentes ;
- F-Secure Anti-Virus for Citrix Servers version 5.50 et versions précédentes ;
- F-Secure Anti-Virus for MIMEsweeper version 5.51 et versions précédentes ;
- F-Secure Anti-Virus Client Security version 5.55 et versions précédentes ;
- F-Secure Anti-Virus for MS Exchange version 6.31 et versions précédentes ;
- F-Secure Internet Gatekeeper version 6.41 et versions précédentes ;
- F-Secure Anti-Virus for Firewalls version 6.20 et versions précédentes ;
- F-Secure Internet Security 2004 et 2005 ;
- F-Secure Anti-Virus 2004 et 2005 ;
- F-Secure Personal Express version 5.10 et versions précédentes ;
- F-Secure Anti-Virus for Linux Workstations version 4.52 et versions précédentes ;
- F-Secure Anti-Virus for Linux Servers version 4.61 et versions précédentes ;

- F-Secure Anti-Virus for Linux Gateways version 4.61 et versions précédentes ;
- F-Secure Anti-Virus for Samba Servers version 4.60 et versions précédentes ;
- F-Secure Anti-Virus Linux Client Security version 5.01 et versions précédentes ;
- F-Secure Anti-Virus Linux Server Security version 5.01 et versions précédentes ;
- F-Secure Internet Gatekeeper for Linux version 2.06 et versions précédentes.

3 Résumé

Une vulnérabilité présente dans divers produits F-Secure lors du traitement des fichiers compressés au format `ARJ` permet l'exécution de code arbitraire.

4 Description

Une vulnérabilité de type débordement de la mémoire tampon a été découverte dans de nombreux produits F-Secure. Cette vulnérabilité permet à un utilisateur mal intentionné de faire exécuter un code arbitraire sur le système vulnérable au moyen d'un fichier compressé au format `ARJ` malicieusement constitué.

5 Solution

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

6 Documentation

- Site Internet de F-Secure :
  http://www.f-secure.com
- Bulletin de sécurité F-Secure FSC-2005-1 du 10 février 2005 :
  http://www.f-secure.com/security/fsc-2005-1.shtml
- Mise à jour de sécurité du paquetage NetBSD fprot-workstation-bin :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/security/fprot-workstation-bin/README.html

Gestion détaillée du document

11 février 2005 version initiale.
14 février 2005 ajout de la référence au bulletin de sécurité NetBSD.