Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 juin 2007
N° CERTA-2007-AVI-244

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités des produits F-Secure

Gestion du document

Référence	CERTA-2007-AVI-244
Titre	Multiples vulnérabilités des produits F-Secure
Date de la première version	01 juin 2007
Date de la dernière version	–
Source(s)	Bulletins de mise à jour F-Secure du 30 mai 2007
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 ;
- déni de service à distance ;
- élévation de privilèges.

2 Systèmes affectés

- F-Secure Anti-virus 2005 ;
- F-Secure Anti-virus 2006 ;
- F-Secure Anti-virus 2007 ;
- F-Secure Anti-virus 5.x ;
- F-Secure Anti-virus Client Security 6.x ;
- F-Secure Anti-virus Client Security 7.x ;
- F-Secure Anti-virus for Citrix Servers 5.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 Windows Servers 5.x ;

- F-Secure Anti-virus for Windows Servers 7.x ;
- F-Secure Anti-virus for Workstation 5.x ;
- F-Secure Anti-virus for Workstation 7.x ;
- F-Secure Anti-virus Linux Client Security 5.x ;
- F-Secure Anti-virus Linux Server Security 5.x ;
- F-Secure Internet Gatekeeper 6.x ;
- F-Secure Internet Gatekeeper for Linux 2.x ;
- F-Secure Internet Security 2005 ;
- F-Secure Internet Security 2006 ;
- F-Secure Internet Security 2007.

3 Résumé

De multiples vulnérabilités touchent les produits anti-virus de l'éditeur `F-Secure`. L'exploitation de ces vulnérabilités permet de réaliser de nombreuses actions malveillantes, allant du déni de service à l'exécution de code arbitraire à distance.

4 Description

Trois vulnérabilités ont été découvertes dans les produits anti-virus de l'éditeur F-Secure :
- la première est due à un mauvais traitement des archives au format `LHA`, entrainant un débordement de mémoire. Cette vulnérabilité peut être exploitée via une archive spécialement construite afin d'exécuter du code arbitraire à distance ;
- la deuxième est due au mauvais traitement de certaines archives ou certains exécutables compressés, entrainant une boucle infinie. Cette vulnérabilité peut être exploitée via une archive ou un exécutable spécialement construit afin de causer un déni de service à distance de l'antivirus ;
- la troisième est due à une erreur dans le module d'analyse en temps-réel. Cette vulnérabilité peut être exploitée à distance afin d'exécuter du code avec des privilèges élevés.

5 Solution

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

6 Documentation

- Site de l'éditeur :
  http://www.f-secure.com
- Bulletin de sécurité FSC-2007-2 du 30 mai 2007 :
  http://www.f-secure.com/security/fsc-2007-2.shtml
- Bulletin de sécurité FSC-2007-3 du 30 mai 2007 :
  http://www.f-secure.com/security/fsc-2007-3.shtml
- Bulletin de sécurité FSC-2007-4 du 30 mai 2007 :
  http://www.f-secure.com/security/fsc-2007-4.shtml
- Référence CVE CVE-2007-2965 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2965
- Référence CVE CVE-2007-2966 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2966
- Référence CVE CVE-2007-2967 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2967

Gestion détaillée du document

01 juin 2007 version initiale.