

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des antivirus Kaspersky et 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-2005-AVI-391>

Gestion du document

Référence	CERTA-2005-AVI-391
Titre	Vulnérabilité des antivirus Kaspersky et F-Secure
Date de la première version	11 octobre 2005
Date de la dernière version	–
Source(s)	Avis de sécurité d'iDefense du 10 octobre 2005
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

- Déni de service sur le filtrage antiviral,
- exécution de code arbitraire à distance.

2 Systèmes affectés

- *Kaspersky Personal 5.x*,
- *Kaspersky Anti-Virus On-Demand Scanner for Linux 5.x*,
- *F-Secure Anti-Virus Linux 4.x*.

3 Résumé

Un utilisateur mal intentionné peut soumettre au moteur d'analyse antivirus un fichier volontairement mal formé provoquant un déni de service voire l'exécution de code arbitraire avec les droits du programme.

4 Description

Le moteur antivirus possède la capacité d'analyser divers formats de fichiers. Parmi ceux-ci, le type CHM (« Compiled HTML Help », format utilisé par les fichiers d'aide *Windows*) peut être utilisé pour provoquer un débordement de tampon dans la pile.

Le moteur de *Kaspersky* est utilisé par d'autres éditeurs, notamment pour les versions Linux qui peuvent être utilisées sur des serveurs de messagerie, de partage de fichiers,...

Un déni de service peut être un moyen préliminaire à la diffusion de code malveillant qui aurait été sinon détecté.

5 Solution

Toute mise à jour de la base de signature postérieure à juillet 2005 corrige cette faille.

6 Documentation

- Avis de sécurité d'iDefense du 10 octobre 2005 :
<http://www.iddefense.com/application/poi/display?id=318&type=vulnerabilities>
- Référence CVE CAN-2005-2937 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2937>

Gestion détaillée du document

11 octobre 2005 version initiale.