Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 janvier 2007
N° CERTA-2007-AVI-009

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'antivirus Kaspersky

Gestion du document

Référence	CERTA-2007-AVI-009
Titre	Vulnérabilité de l'antivirus Kaspersky
Date de la première version	08 janvier 2007
Date de la dernière version	–
Source(s)	Avis iDefense 459
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 à distance.

2 Systèmes affectés

- *Kaspersky Labs Antivirus Engine version 6* pour *Windows* ;
- *Kaspersky Labs Antivirus Engine version 5.5-10* pour *Linux*.

3 Résumé

Un traitement défectueux des fichiers exécutables permet à un utilisateur malveillant de réaliser un déni de service à distance.

4 Description

Kaspersky Labs Antivirus Engine est un antivirus utilisable sur le poste de travail ou sur une passerelle de messagerie. Un fichier exécutable pour *Windows* au format PE contient une section d'en-tête utilisée pour le chargeur et l'éditeur de lien, section nommée *Optional Windows Header section*. Une valeur invalide dans le

champ `NumberOfRvaAndSizes` permet de provoquer une boucle infinie. Le manque de validation de ce champ permet à un utilisateur malintentionné de provoquer un déni de service à distance.

5 Solution

Utiliser le système de mise à jour automatique de l'éditeur.

6 Documentation

– Bulletin de sécurité iDefense du 05 janvier 2007 :
http://www.idefense.com/application/poi/display?id=459

Gestion détaillée du document

08 janvier 2007 version initiale.