



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 04 octobre 2005  
N° CERTA-2005-AVI-378

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de l'antivirus Kaspersky

---

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-378>

---

### Gestion du document

Référence	CERTA-2005-AVI-378
Titre	Vulnérabilité de l'antivirus Kaspersky
Date de la première version	04 octobre 2005
Date de la dernière version	–
Source(s)	Note d'information de Kaspersky
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 ;
- exécution de code arbitraire.

## 2 Systèmes affectés

Toutes les versions de Kaspersky disponibles pour les systèmes d'exploitation Microsoft Windows.

## 3 Description

Un mauvais traitement des fichiers \*.cab provoque un dépassement de mémoire permettant à un utilisateur mal-intentionné d'obtenir le contrôle total de la machine cible.

Cette vulnérabilité peut être exploitée sans action d'un utilisateur, à travers les protocoles courants tels que SMTP, SMB, HTTP, et FTP.

## **4 Contournement provisoire**

Kaspersky a intégré dans ses bases une signature permettant de reconnaître et de supprimer un fichier CAB malicieusement construit. La base de signature doit donc être mise à jour si celle-ci est antérieure au 29 septembre 2005.

## **5 Solution**

Un patch correctif sera disponible sur le site de l'éditeur à compter du 05 octobre 2005.

## **6 Documentation**

- Note d'information de Kaspersky :  
<http://www.kaspersky.com/news?id=171512144>
- Bulletin de sécurité de rem0te.com :  
<http://www.rem0te.com/public/images/kaspersky.pdf>

## **Gestion détaillée du document**

**04 octobre 2005** version initiale.