

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des produits 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-2007-AVI-161>

Gestion du document

Référence	CERTA-2007-AVI-161
Titre	Vulnérabilité des produits Kaspersky
Date de la première version	05 avril 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité Kaspersky #203038693 et #203038694 du 05 avril 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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Kaspersky Anti-Virus 4.x ;
- Kaspersky Anti-Virus 5.x ;
- Kaspersky Anti-Virus 6.x ;
- Kaspersky Internet Security 6.x.

3 Résumé

De multiples vulnérabilités dans les produits antivirus de Kaspersky permettent à un utilisateur distant de porter atteinte à la confidentialité des données, de provoquer un déni de service, d'exécuter du code arbitraire.

4 Description

Plusieurs vulnérabilités sont présentes dans les produits antivirus de Kaspersky :

- la première concerne un manque de vérification par des contrôles ActiveX fournis avec les produits Kaspersky. Ceci permet à un utilisateur distant d'obtenir des fichiers présents sur le système vulnérable via un site web particulier ;
- la deuxième vulnérabilité est présente dans le fichier `klif.sys` et permet l'exécution de code arbitraire à distance ;
- la dernière concerne la mise en œuvre du support des fichiers de type ARJ et permet l'exécution de code arbitraire au moyen d'un fichier `.arj` particulier.

5 Solution

La version 6.0.2.614 corrige le problème. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

Bulletins de sécurité Kaspersky #203038693 et #203038694 du 05 avril 2007 :

<http://www.kaspersky.com/technews?id=203038693>

<http://www.kaspersky.com/technews?id=203038694>

Gestion détaillée du document

05 avril 2007 version initiale.