

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Kaspersky Anti-Virus

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-2006-AVI-460>

Gestion du document

Référence	CERTA-2006-AVI-460
Titre	Vulnérabilité dans Kaspersky Anti-Virus
Date de la première version	24 octobre 2006
Date de la dernière version	–
Source(s)	Avis de sécurité iDefense #425 du 19 octobre 2006
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Kaspersky Anti-Virus Personal 5.0 ;
- Kaspersky Anti-Virus Personal Pro 5.0 ;
- Kaspersky Anti-Virus 5.0 pour stations Windows ;
- Kaspersky Anti-Virus 6.0 ;
- Kaspersky Internet Security 6.0.

3 Résumé

Une vulnérabilité a été identifiée dans certains produits Kaspersky. Exploitée, celle-ci permettrait à une personne malveillante locale de désactiver l'antivirus, voire d'exécuter des commandes arbitraires sur le système avec les droits de l'administrateur.

4 Description

Une vulnérabilité a été identifiée dans certains produits Kaspersky. Elle proviendrait d'une mauvaise manipulation de l'espace d'adressage effectuée par les pilotes `KLIN` et `CLICK`. Une personne malveillante pourrait exploiter cette vulnérabilité, afin de désactiver l'antivirus, voire d'exécuter des commandes arbitraires sur le système avec les droits de l'administrateur.

5 Solution

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

6 Documentation

- Référence CVE CVE-20064926 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-20064926>
- Bulletin de sécurité iDefense #425 du 19 octobre 2006 :
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=425>
- Annonce Kaspersky du 20 octobre 2006 :
<http://www.kaspersky.com/technews?id=203038678>

Gestion détaillée du document

24 octobre 2006 version initiale.