



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 23 novembre 2006  
N° CERTA-2006-AVI-511

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de CA personal Firewall

---

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-511>

---

### Gestion du document

Référence	CERTA-2006-AVI-511
Titre	Vulnérabilité de CA personal Firewall
Date de la première version	23 novembre 2006
Date de la dernière version	–
Source(s)	
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

Élévation de privilèges.

## 2 Systèmes affectés

– CA Personal Firewall 2007 9.x.

## 3 Résumé

Des erreurs dans des pilotes du pare-feu permettent à un utilisateur local d'élever ses privilèges.

## 4 Description

Des erreurs affectent les pilotes `KmxStart.sys` et `KmxFw.sys` du pare-feu personnel de CA. Ces erreurs peuvent être utilisées par un utilisateur local pour modifier des fonctions de retour (*callbacks*) via des primitives `IOCTL` privilégiées. L'utilisateur malveillant peut alors exécuter un code arbitraire dans l'espace noyau (*kernel mode*).

Les vulnérabilités sont avérées pour les versions suivantes des pilotes :

- KmxStart.sys 6.5.4.10
- KmxFw.sys 6.5.4.31

## **5 Contournement provisoire**

Restreindre aux utilisateurs autorisés l'accès aux systèmes vulnérables.

## **6 Documentation**

- Avis de sécurité Secunia SA22972 du 17 novembre 2006 :  
<http://secunia.com/advisories/22972/>

## **Gestion détaillée du document**

**23 novembre 2006** version initiale.