



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 12 août 2008  
N° CERTA-2008-AVI-401

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Plusieurs vulnérabilités dans des produits CA

---

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-2008-AVI-401>

---

### Gestion du document

Référence	CERTA-2008-AVI-401
Titre	Plusieurs vulnérabilités dans des produits CA
Date de la première version	12 août 2008
Date de la dernière version	–
Source(s)	Avis de sécurité CA 36559 et 36560 du 11 août 2008
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 ;
- déni de service à distance à distance.

## 2 Systèmes affectés

- CA Host-Based Intrusion Prevention System r8 ;
- CA Internet Security Suite 2007 ;
- CA Internet Security Suite 2008 ;
- CA Personal Firewall 2007 ;
- CA Personal Firewall 2008.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans des produits de sécurité CA. Elles permettraient à des personnes locales d'exécuter du code arbitraire ou de perturber à distance le fonctionnement du service.

## 4 Description

Plusieurs vulnérabilités ont été identifiées dans des produits de sécurité CA. Elles permettraient à des personnes locales d'exécuter du code arbitraire ou de perturber à distance le fonctionnement du système. Ces vulnérabilités affectent le pilote `kmxfw.sys`.

## 5 Solution

Se référer aux bulletins de sécurité de CA pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Avis de sécurité CA 36559 du 12 août 2008 :  
<http://www.ca.com/us/securityadvisor/vulninfo/vuln.aspx?id=36559>
- Avis de sécurité CA 36560 du 12 août 2008 :  
<http://www.ca.com/us/securityadvisor/vulninfo/vuln.aspx?id=36560>
- Référence CVE CVE-2008-2926 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2926>
- Référence CVE CVE-2008-3174 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3174>

## Gestion détaillée du document

12 août 2008 version initiale.