

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de produits Computer Associates

---

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-252>

---

### Gestion du document

Référence	CERTA-2007-AVI-252
Titre	Multiples vulnérabilités de produits Computer Associates
Date de la première version	06 juin 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA du 05 juin 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.

## 2 Systèmes affectés

- CA Anti-Virus for the Enterprise r8, r8.1 ;
- CA Anti-Virus 2007 (v8) ;
- eTrust EZ Antivirus r7, r6.1 ;
- CA Internet Security Suite 2007 (v3) ;
- eTrust Internet Security Suite r1, r2 ;
- eTrust EZ Armor r1, r2, r3.x ;
- CA Threat Manager for the Enterprise r8 ;
- CA Protection Suites r2, r3 ;
- CA Secure Content Manager 8.0 ;
- CA Anti-Virus Gateway 7.1 ;
- Unicenter Network and Systems Management (NSM) r3.0 ;

- *Unicenter Network and Systems Management (NSM) r3.1 ;*
- *Unicenter Network and Systems Management (NSM) r11 ;*
- *Unicenter Network and Systems Management (NSM) r11.1 ;*
- *BrightStor ARCserve Backup r11.5 ;*
- *BrightStor ARCserve Backup r11.1 ;*
- *BrightStor ARCserve Backup r11 for Windows ;*
- *BrightStor Enterprise Backup r10.5 ;*
- *BrightStor ARCserve Backup v9.01 ;*
- *CA Common Services ;*
- *CA Anti-Virus SDK.*

### **3 Résumé**

Des vulnérabilités permettent à des utilisateurs malintentionnés de provoquer un déni de service à distance et potentiellement une exécution de code arbitraire à distance.

### **4 Description**

Deux vulnérabilités ont été trouvées dans le traitement des fichiers de type CAB :

- l'une est due à la mauvaise gestion des noms de fichiers excessivement longs contenus dans le fichier CAB ;
- l'autre est liée à la validation insuffisante du champ `coFFiLe` dans un fichier CAB .

Ces deux vulnérabilités permettent de provoquer un arrêt brutal du programme et potentiellement d'exécuter un code arbitraire à distance.

### **5 Solution**

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

### **6 Documentation**

- Bulletin de sécurité Computer Associates du 05 juin 2007 :  
<http://supportconnectw.ca.com/public/antivirus/infodocs/caantivirus-securitynotice.asp>
- Référence CVE CVE-2007-2863 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2863>
- Référence CVE CVE-2007-2864 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2864>

### **Gestion détaillée du document**

**06 juin 2007** version initiale.