



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 juillet 2007
N° CERTA-2007-AVI-329

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans plusieurs 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-329>

Gestion du document

Référence	CERTA-2007-AVI-329
Titre	Vulnérabilités dans plusieurs produits Computer Associates
Date de la première version	25 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Computer Associates du 24 juillet 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

Déni de service à distance.

2 Systèmes affectés

- CA Anti-Virus for the Enterprise (anciennement eTrust Antivirus) 7.0, 7.1, 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 (anciennement eTrust Integrated Threat Management) r8 ;
- CA Anti-Virus Gateway (anciennement eTrust Antivirus Gateway) 7.1 ;
- CA Protection Suites r2, r3 ;
- CA Secure Content Manager (anciennement eTrust Secure Content Manager) 1.1, 8.0 ;
- CA Anti-Spyware for the Enterprise (anciennement eTrust PestPatrol) r8, 8.1 ;
- CA Anti-Spyware 2007 ;
- Unicenter Network and Systems Management (NSM) r3, 3.1, r11, r11.1 ;

- *BrightStor ARCserve Backup* r11 pour Windows, r11.1, r11.5 ;
- *BrightStor Enterprise Backup* r10.5 ;
- *BrightStor ARCserve Backup* v9.01 ;
- *BrightStor ARCserve Client agent for Windows* ;
- *eTrust Intrusion Detection* 2.0 SP1, 3.0, 3.0 SP1 ;
- *CA Common Services (CCS)* r11, r11.1 ;
- *CA Anti-Virus SDK* (anciennement *eTrust Anti-Virus SDK*).

3 Résumé

Deux vulnérabilités affectant la bibliothèque `arclib.dll` permettent de réaliser un déni de service à distance.

4 Description

Deux vulnérabilités affectant la bibliothèque `arclib.dll` (versions antérieures à 7.3.0.9), présente dans de nombreux produits de l'éditeur *Computer Associates*, ont été découvertes. Ces vulnérabilités permettent, par le biais d'un fichier au format CHM (CVE-2007-3875) ou au format RAR (CVE-2006-5645) spécifiquement constitué, de réaliser un déni de service 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 24 juillet 2007 :
<http://supportconnectw.ca.com/public/antivirus/infodocs/caprodarclib-sectnot.asp>
- Référence CVE-2006-5645 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5645>
- Référence CVE-2007-3875 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3875>

Gestion détaillée du document

25 juillet 2007 version initiale.