



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 octobre 2009
N° CERTA-2009-AVI-431

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans CA 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-2009-AVI-431>

Gestion du document

Référence	CERTA-2009-AVI-431
Titre	Vulnérabilités dans CA Anti-Virus
Date de la première version	12 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA20091008-01 du 08 octobre 2009
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 (autrefois appelé *eTrust Antivirus*) 7.1, r8 et r8.1 ;
- CA Anti-Virus 2007 (v8) ;
- CA Anti-Virus 2008 ;
- CA Anti-Virus 2009 ;
- CA Anti-Virus Plus 2009 ;
- *eTrust EZ Antivirus* r7.1 ;
- CA Internet Security Suite 2007 (v3) ;
- CA Internet Security Suite 2008 ;
- CA Internet Security Suite Plus 2008 ;
- CA Internet Security Suite Plus 2009 ;
- CA Threat Manager for the Enterprise (autrefois appelé *eTrust Integrated Threat Management*) r8 et 8.1 ;
- CA Threat Manager Total Defense ;

- *CA Gateway Security* r8.1 ;
- *CA Protection Suites* r2, r3 et r3.1 ;
- *CA Secure Content Manager* (autrefois appelé *eTrust Secure Content Manager*) 1.1 et 8.0 ;
- *CA Network and Systems Management* (autrefois appelé *Unicenter Network and Systems Management*) r3.0, r3.1, r11, r11.1 ;
- *CA ARCserve Backup* pour *Windows* r11.5, r12, r12.0 SP1, r12.0 SP2 et r12.5 ;
- *CA ARCserve Backup* pour *Linux* r11.1 et r11.5 ;
- *CA ARCserve for Windows Client Agent* ;
- *CA ARCserve for Windows Server component* ;
- *CA eTrust Intrusion Detection 2.0* SP1, 3.0 et 3.0 SP1 ;
- *CA Common Services* r3.1, r11 et r11.1 ;
- *CA Anti-Virus SDK* (autrefois appelé *eTrust Anti-Virus SDK*) ;
- *CA Anti-Virus Gateway* (autrefois appelé *eTrust Antivirus Gateway*) 7.1.

3 Résumé

Deux vulnérabilités dans *CA Anti-Virus* permettent d'exécuter du code arbitraire ou de réaliser un déni de service à distance.

4 Description

Deux vulnérabilités ont été découvertes dans le traitement des fichiers au format RAR par le composant *arclib* de *CA Anti-Virus*. L'exploitation de ces vulnérabilités permet de réaliser un déni de service ou d'exécuter du 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 CA20091008-01 du 08 octobre 2009 :
<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=218878>
- Référence CVE CVE-2009-3587 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3587>
- Référence CVE CVE-2009-3588 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3588>

Gestion détaillée du document

12 octobre 2009 version initiale.