



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 janvier 2009
N° CERTA-2009-AVI-033

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-033>

Gestion du document

Référence	CERTA-2009-AVI-033
Titre	Multiples vulnérabilités dans CA Anti-Virus
Date de la première version	28 janvier 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA20090126-01 du 26 janvier 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

Contournement de la politique de sécurité.

2 Systèmes affectés

- CA Anti-Virus for the Enterprise (autrefois appelé *eTrust Antivirus*) versions 7.1, r8 et r8.1 ;
- CA Anti-Virus 2007 version v8 ;
- CA Anti-Virus 2008 ;
- *eTrust EZ Antivirus* versions r7 et r6.1 ;
- CA Internet Security Suite 2007 version v3 ;
- CA Internet Security Suite 2008 ;
- CA Threat Manager for the Enterprise (autrefois appelé *eTrust Integrated Threat Management*) versions r8 et r8.1 ;
- CA Anti-Virus Gateway (autrefois appelé *eTrust Antivirus Gateway*) version 7.1 ;
- CA Protection Suites versions r2, r3 et r3.1 ;
- CA Secure Content Manager (autrefois appelé *eTrust Secure Content Manager*) versions 8.0 et 8.1 ;
- CA Anti-Spyware for the Enterprise (autrefois appelé *eTrust PestPatrol*) versions r8 et r8.1 ;
- CA Anti-Spyware 2007 ;

- *CA Anti-Spyware 2008* ;
- *CA Network and Systems Management* (autrefois appelé *Unicenter Network and Systems Management* versions r3.0, r3.1, r11 et r11.1 ;
- *CA ARCserve Backup* versions r11.1, r11.5 et r12 pour Windows ;
- *CA ARCserve Backup* versions r11.1 et r11.5 pour Linux ;
- *CA ARCserve client agent for Windows* ;
- *CA eTrust Intrusion Detection* versions 2.0 SP1, 3.0, 3.0 SP1 et 4.0 ;
- *CA Common Services* versions r11, r11.1 ;
- *CA Anti-Virus SDK* (autrefois appelé *eTrust Anti-Virus SDK*).

3 Résumé

De multiples vulnérabilités dans *CA Anti-Virus* permettent de contourner le mécanisme de détection des codes malveillants.

4 Description

De multiples vulnérabilités ont été découvertes dans le moteur de *CA Anti-Virus*. À l'aide d'une archive spécifiquement constituée, un utilisateur malintentionné peut contourner le mécanisme de détection des codes malveillants.

5 Solution

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

6 Documentation

- Bulletin de sécurité CA20090126-01 du 26 janvier 2009 :
<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=197601>
- Référence CVE CVE-2009-0042 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0042>

Gestion détaillée du document

28 janvier 2009 version initiale.