



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 17 décembre 2004  
N° CERTA-2004-AVI-403

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité d'eTrust Antivirus de 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-2004-AVI-403>

---

### Gestion du document

Référence	CERTA-2004-AVI-403
Titre	Vulnérabilité d'eTrust Antivirus de Computer Associates
Date de la première version	17 décembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité d'iDEFENSE
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

Elévation de privilèges.

## 2 Systèmes affectés

eTrust EZ Antivirus versions r7.0.0 - r7.0.4.

## 3 Description

Selon l'éditeur Computer Associates, les fichiers du logiciel eTrust EZ Antivirus ne sont pas installés avec des droits d'accès correctement positionnés.

Certains des programmes de l'antivirus s'exécutant avec les privilèges SYSTEM, il est alors possible pour un utilisateur local mal intentionné de modifier ces fichiers pour réaliser une élévation de privilèges.

## 4 Solution

La version r7.0.5 du logiciel corrige cette vulnérabilité.

## 5 Documentation

- Bulletin de sécurité de Computer Associates "Vulnerability ID: 32054 - CA eTrust EZ Antivirus Insecure File Permission" du 15 décembre 2004 :  
<http://crm.my-etrust.com/CIDocument.asp?KDIId=2222&GUID=CF4848E796964617849BA923F9299C98>
- Bulletin de sécurité d'iDEFENSE "Computer Associates eTrust EZ Antivirus Insecure File Permission Vulnerability" du 15 décembre 2004 :  
<http://www.idefense.com/application/poi/display?id=164>
- Référence CVE CAN-2004-1149 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1149>

### Gestion détaillée du document

17 décembre 2004 version initiale.