



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 septembre 2006
N° CERTA-2006-AVI-409

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans CA

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-2006-AVI-409>

Gestion du document

Référence	CERTA-2006-AVI-409
Titre	Vulnérabilités dans CA
Date de la première version	22 septembre 2006
Date de la dernière version	–
Source(s)	
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Computer Associates eTrust Audit version r8 ;
- Computer Associates eTrust Audit version 1.
- Computer Associates eTrust Security Command Center version r8 ;
- Computer Associates eTrust Security Command Center version r8 SP1 CR1 ;
- Computer Associates eTrust Security Command Center version r8 SP1 CR2 ;
- Computer Associates eTrust Security Command Center version 1.0.

3 Résumé

Plusieurs vulnérabilités dans des composants de Computer Associates permettent à des agresseurs de contourner des règles de sécurité et d'accéder à des données sensibles.

4 Description

La première vulnérabilité provient d'une erreur dans le script `ePPIServlet` qui gère incorrectement des paramètres mal formés. Cette vulnérabilité permet à des agresseurs d'obtenir des informations relatives à l'arborescence du système cible (chemin vers le répertoire d'installation).

La seconde vulnérabilité provient d'une erreur dans le script `eSMPAuditServlet` qui valide incorrectement des paramètres. Cette vulnérabilité permet à des agresseurs de lire ou de détruire des fichiers arbitraires.

La troisième vulnérabilité se trouve au niveau du système de gestion des alertes qui est accessible sans authentification préalable. Cette vulnérabilité permet à des agresseurs d'envoyer de fausses alertes.

5 Contournement provisoire

6 Solution

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

7 Documentation

– Bulletin de sécurité de CA :

http://supportconnectw.ca.com/public/etrust/eTrust_scc/downloads/eTrustscc_updates.asp

Gestion détaillée du document

22 septembre 2006 version initiale.