



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 octobre 2008  
N° CERTA-2008-AVI-491

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans CA ARCserve Backup

---

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-2008-AVI-491>

---

### Gestion du document

Référence	CERTA-2008-AVI-491
Titre	Multiples vulnérabilités dans CA ARCserve Backup
Date de la première version	13 octobre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA du 09 octobre 2008
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 ARCserve Backup Windows r12.0 ;
- CA ARCserve Backup Windows r11.5 ;
- CA ARCserve Backup Windows r11.1 ;
- CA Server Protection Suite r2 ;
- CA Business Protection Suite r2 ;
- CA Business Protection Suite for Microsoft Small Business Server Standard Edition r2 ;
- CA Business Protection Suite for Microsoft Small Business Server Premium Edition r2.

## 3 Résumé

Plusieurs vulnérabilités dans CA ARCserve Backup permettent à distance d'exécuter du code arbitraire ou de provoquer des dénis de service.

## 4 Description

Quatre vulnérabilités ont été découvertes dans *CA ARCserve Backup* :

- une validation insuffisante des paramètres passés à certains appels RPC permet d'exécuter du code arbitraire à distance (CVE-2008-4397) ;
- une faille dans le service `tape engine` permet de réaliser un déni de service à distance (CVE-2008-4398) ;
- une vulnérabilité dans le service `database engine` permet de réaliser un déni de service à distance (CVE-2008-4399) ;
- une vérification incorrecte des identifiants de connexion permet de réaliser plusieurs dénis de service (CVE-2008-4400).

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité CA du 09 octobre 2008 :  
<http://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=188143>
- Référence CVE CVE-2008-4397 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4397>
- Référence CVE CVE-2008-4398 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4398>
- Référence CVE CVE-2008-4399 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4399>
- Référence CVE CVE-2008-4400 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4400>

## Gestion détaillée du document

13 octobre 2008 version initiale.