Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 mars 2007
N° CERTA-2007-AVI-133

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans BrightStor ARCserve

Gestion du document

Référence	CERTA-2007-AVI-133
Titre	Vulnérabilités dans BrightStor ARCserve
Date de la première version	16 mars 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité de CA du 15 mars 2007
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

- BrightStor ARCserve Backup r11.5 ;
- BrightStor ARCserve Backup r11.1 ;
- BrightStor ARCserve Backup r11 for Windows ;
- BrightStor Enterprise Backup r10.5 ;
- BrightStor ARCserve Backup r9.01 ;
- 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

Quatre vulnérabilités dans `BrightStor ARCserve` peuvent être exploitées par une personne malintentionnée distante afin d'effectuer un déni de service ou une exécution de code arbitraire.

4 Description

Quatre vulnérabilités ont été identifiées dans `BrightStor ARCserve` :

- un débordement de tampon possible dans le service `Tape Engine` qui permet l'exécution de code arbitraire ;
- une corruption de mémoire dans le traitement de procédures `RPC` par le service `Tape Engine` qui cause un déni de service et potentiellement l'exécution de code arbitraire ;
- un mauvais traitement de paramètres par le service `catirpc.dll` qui permet à un attaquant d'envoyer des requêtes malformées pour causer un déni de service ;
- une fonction `RPC`, pouvant être appelée par une personne malintentionnée distante, qui éteint le service `Tape Engine`.

5 Solution

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

6 Documentation

- Référence CVE CVE-2006-6076 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6076
- Référence CVE CVE-2007-0816 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0816
- Référence CVE CVE-2007-1447 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1447
- Référence CVE CVE-2007-1448 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1448
- Bulletin de sécurité de CA du 15 mars 2007 :
  http://supportconnecttw.ca.com/public/storage/infodocs/babtapeng-securitynotice.asp

Gestion détaillée du document

16 mars 2007 version initiale.