



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 octobre 2007
N° CERTA-2007-AVI-437

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans BrightStor 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-2007-AVI-437>

Gestion du document

Référence	CERTA-2007-AVI-437
Titre	Multiples vulnérabilités dans BrightStor ARCserve Backup
Date de la première version	12 octobre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Computer Associates du 11 octobre 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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- *BrightStor ARCserve Backup* r11.5 ;
- *BrightStor ARCserve Backup* r11.1 ;
- *BrightStor ARCserve Backup* r11 pour Windows ;
- *BrightStor Enterprise Backup* r10.5 ;
- *BrightStor ARCserve Backup* v9.01 ;
- *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

Plusieurs vulnérabilités dans *BrightStor ARCserve Backup* permettent, à distance, d'exécuter du code arbitraire, de réaliser un déni de service ou de contourner la politique de sécurité.

4 Description

Plusieurs failles ont été découvertes dans *BrightStor ARCserve Backup* :

- des vulnérabilités, de type débordement de mémoire, permettent d'exécuter du code arbitraire à distance (CVE-2007-5325, CVE-2007-5326 et CVE-2007-5327) ;
- un utilisateur peut accéder à des fonctionnalités nécessitant théoriquement des privilèges élevés (CVE-2007-5328) ;
- plusieurs problèmes dans la gestion des procédures RPC par différents services permettent de réaliser un déni de service. La possibilité d'exécuter du code arbitraire n'est pas exclue (CVE-2007-5329, CVE-2007-5330, CVE-2007-5331 et CVE-2007-5332).

5 Solution

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

6 Documentation

- Bulletin de sécurité Computer Associates du 11 octobre 2007 :
<http://supportconnectw.ca.com/public/storage/infodocs/basb-secnotice.asp>
- Référence CVE CVE-2007-5325 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5325>
- Référence CVE CVE-2007-5326 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5326>
- Référence CVE CVE-2007-5327 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5327>
- Référence CVE CVE-2007-5328 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5328>
- Référence CVE CVE-2007-5329 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5329>
- Référence CVE CVE-2007-5330 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5330>
- Référence CVE CVE-2007-5331 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5331>
- Référence CVE CVE-2007-5332 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5332>

Gestion détaillée du document

12 octobre 2007 version initiale.