

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité 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-ALE-009>

Gestion du document

Référence	CERTA-2007-ALE-009-001
Titre	Vulnérabilité dans BrightStor ARCserve Backup
Date de la première version	30 mars 2007
Date de la dernière version	27 avril 2007
Source(s)	Bulletin de sécurité Secunia SA24682 du 30 mars 2007 Bulletin de sécurité Computer Associates du 24 avril 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.

2 Systèmes affectés

BrightStor ARCserve Backup versions 11.5 SP2 build 4237 et antérieures.

3 Résumé

Une vulnérabilité dans BrightStor ARCserve Backup permettrait à un utilisateur distant d'exécuter du code arbitraire sur la machine vulnérable.

4 Description

Un manque de contrôle des requêtes RPC (Remote Procedure Call) passées au composant `mediasvr.exe` de BrightStor ARCserve Backup permettrait à un utilisateur distant mais provenant du même réseau

d'exécuter du code arbitraire par le biais d'une requête RPC construite de façon particulière. Il existe une preuve de faisabilité mettant en œuvre cette vulnérabilité sur l'Internet.

Cette vulnérabilité a été corrigée et a fait l'objet de l'avis CERTA-2007-AVI-188.

5 Contournement provisoire

Dans la mesure où cette vulnérabilité offre à l'attaquant la possibilité de contrôler la machine à distance, il convient de :

- ne pas rendre accessible depuis l'Internet la machine mettant en œuvre BrightStor ARCserve Backup ;
- restreindre l'accès au service mediasvr.exe aux seules machines autorisées à dialoguer via RPC avec lui.

6 Solution

Se référer au bulletin de sécurité de l'éditeur (voir Documentation).

7 Documentation

- Bulletin de sécurité Computer Associates du 24 avril 2007 :
<http://supportconnectw.ca.com/public/storage/infodocs/babmedser-secnotice.asp>
- Avis CERTA-2007-AVI-188 du 25 avril 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-188/>
- Bulletin de sécurité Secunia SA24682 du 30 mars 2007 :
<http://www.secunia.com/advisories/24682>
- Référence CVE CVE-2007-1785 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1785>
- Référence CVE CVE-2007-2139 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2139>

Gestion détaillée du document

30 mars 2007 version initiale.

27 avril 2007 ajout de la section Solution, des références au bulletin de sécurité Computer Associates et des entrées CVE.