

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans BrightStor ARCserve

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-2005-AVI-143>

Gestion du document

Référence	CERTA-2005-AVI-143-001
Titre	Vulnérabilité dans BrightStor ARCserve
Date de la première version	14 avril 2005
Date de la dernière version	15 avril 2005
Source(s)	Bulletins de sécurité Computer Associates du 08 avril 2005
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 r11.1 ;
- BrightStor ARCserve Backup Client Agent r11.1 ;
- BrightStor ARCserve Backup r11.0 ;
- BrightStor ARCserve Backup v9.01 ;
- BrightStor ARCserve Backup Client Agent v9.01 ;
- BrightStor ARCserve Backup v10.5 ;
- BrightStor ARCserve Backup v10.0.

3 Résumé

Une vulnérabilité de type débordement de mémoire dans BrightStor ARCserve Backup UniversalAgent permet l'exécution de code arbitraire à distance.

4 Description

BrightStor ARCserve Backup est un serveur de sauvegarde. Il utilise un agent réseau qui écoute par défaut sur le port 6050 (TCP et UDP).

Un utilisateur mal intentionné peut, par le biais d'un paquet TCP malicieusement constitué envoyé à cet agent, exécuter du code arbitraire à distance avec les droits de l'administrateur sur le serveur BrightStor ARCserve Backup.

5 Contournement provisoire

Filtrer le port 6050 (TCP et UDP) au niveau du pare-feu.

6 Solution

Appliquer le correctif de Computer Associates (cf. Documentation).

7 Documentation

- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r11.1 pour Windows :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66526&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r11.1 pour Window64-Bit Edition :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66534&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r11.Client Agent 1 pour Windows :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66527&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r11.0 pour Windows :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66525&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r11.0 pour Windows 64-Bit Edition :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66535&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r9.01 pour Windows (versions anglaises) :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66528&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r9.01 pour Windows (versions non-anglaises) :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66529&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r9.01 pour Windows 64-Bit Edition :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66536&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r9.01 Client Agent pour Windows (versions anglaises) :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66530&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r9.01 Client Agent pour Windows (versions non-anglaises) :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66531&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r10.5 pour Windows :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66524&os=NT>
- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r10.5 pour Windows 64-Bit Edition :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66533&os=NT>

- Bulletin de sécurité Computer Associates du 08 avril 2005 pour BrightStor ARCserve Backup r10.0 pour Windows :
<http://supportconnect.ca.com/sc/solcenter/soldetail.jsp?aparno=QO66523&os=NT>
- Bulletin de sécurité Computer Associates du 11 avril 2005 :
<http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=32727>
- Référence CVE CAN-2005-1018 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1018>

Gestion détaillée du document

14 avril 2005 version initiale.

15 avril 2005 ajout de la référence CVE et de l'avis de Computer Associates.