



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 août 2005
N° CERTA-2005-AVI-293

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans BrightStor ARCserve/Enterprise Backup Agents

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-293>

Gestion du document

Référence	CERTA-2005-AVI-293
Titre	Vulnérabilité dans BrightStor ARCserve/Enterprise Backup
Date de la première version	03 août 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité 33239 de Computer Associates du 02 août 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 r11.0 ;
- BrightStor ARCserve Backup v9.01 ;
- BrightStor Enterprise Backup v10.5 ;
- BrightStor Enterprise Backup v10.0.

3 Résumé

Une vulnérabilité dans les agents de BrightStor ARCserve Backup et de BrightStor Enterprise Backup permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire a été découverte dans les agents SQL, Oracle et SAP R/3 des produits BrightStor ARCserve Backup et BrightStor Enterprise Backup pour Windows. Un utilisateur mal intentionné peut, par le biais de paquets malicieusement construits envoyés au port 6070/tcp, exécuter du code arbitraire à distance sur le serveur.

5 Solution

Appliquer le correctif tel qu'indiqué dans le bulletin de sécurité 33239 de Computer Associates (voir section Documentation).

6 Documentation

- Bulletin de sécurité 33239 de Computer Associates du 02 août 2005 :
<http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=33239>
- Référence CVE CAN-2005-1272 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1272>

Gestion détaillée du document

03 août 2005 version initiale.