



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 24 septembre 2007  
N° CERTA-2007-AVI-415

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans les produits CA 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-2007-AVI-415>

---

### Gestion du document

Référence	CERTA-2007-AVI-415
Titre	Multiples vulnérabilités dans les produits CA ARCserve
Date de la première version	24 septembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA ARCserve du 21 septembre 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

- CA ARCserve Backup for Laptops and Desktops r11.5 ;
- CA ARCserve Backup for Laptops and Desktops r11.1 SP2 ;
- CA ARCserve Backup for Laptops and Desktops r11.1 SP1 ;
- CA ARCserve Backup for Laptops and Desktops r11.1 ;
- CA ARCserve Backup for Laptops and Desktops r11.0 ;
- CA ARCserve Backup for Laptops and Desktops r4.0 ;
- CA Desktop Management Suite 11.2 ;
- CA Desktop Management Suite 11.1 ;
- CA Desktop Management Suite 11.0 ;
- CA Protection Suite r2.

### 3 Résumé

De multiples vulnérabilités dans les produits ARCserve de Computer Associate permettent à un utilisateur distant d'exécuter du code arbitraire.

### 4 Description

Plusieurs vulnérabilités sont présentes dans les produits ARCserve Backup for Laptops and Desktops de Computer Associates. Ces vulnérabilités sont toutes relatives à un manque de contrôle dans les éléments suivants du logiciel :

- le service LGServer ;
- le service d'authentification de ARCserve Backup ;
- le service d'authentification rxLogin ;
- le service NetBackup lors d'un téléchargement de fichier.

### 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 :  
<http://supportconnectw.ca.com/public/sams/lifeguard/infodocs/caarcservebld-securitynotice.asp>
- Bulletin de sécurité iDefense du 21 septembre 2007 :  
<http://www.iddefense.com/application/poi/display?id=598>
- Bulletin de sécurité iDefense du 21 septembre 2007 :  
<http://www.iddefense.com/application/poi/display?id=599>
- Référence CVE CVE-2007-3216 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3216>
- Référence CVE CVE-2007-5003 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5003>
- Référence CVE CVE-2007-5004 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5004>
- Référence CVE CVE-2007-5005 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5005>
- Référence CVE CVE-2007-5006 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5006>

### Gestion détaillée du document

24 septembre 2007 version initiale.