Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 mai 2008
N° CERTA-2008-AVI-258

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans CA ARCserve Backup

Gestion du document

Référence	CERTA-2008-AVI-258
Titre	Vulnérabilités dans CA ARCserve Backup
Date de la première version	21 mai 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA #17698 du 19 mai 2008
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.

2 Systèmes affectés

- CA ARCserve Backup r11.5 ;
- CA ARCserve Backup r11.1 ;
- CA ARCserve Backup r11.0 ;
- 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

Deux vulnérabilités dans *CA ARCserve Backup* permettent à une personne malintentionnée distante de réaliser un déni de service ou d'exécuter du code arbitraire.

4 Description

Deux vulnérabilités ont été identifiées dans *CA ARCserve Backup*. La première est due à une mauvaise vérification de chemin par le service de journalisation `caloggerd`, ce qui permet à une personne malintentionnée d'ajouter des données à des fichiers arbitraires. La deuxième vulnérabilité est due à un débordement de mémoire ce qui permet à une personne malintentionnée d'exécuter du code arbitraire.

5 Solution

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

6 Documentation

- Bulletin de sécurité CA #176798 du 19 mai 2008 :
  https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=176798
- Référence CVE CVE-2008-2241 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2241
- Référence CVE CVE-2008-2242 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2242

Gestion détaillée du document

21 mai 2008 version initiale.