

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Symantec Backup Exec

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-303>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2007-AVI-303 |
| Titre | Vulnérabilité dans Symantec Backup Exec |
| Date de la première version | 12 juillet 2007 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Symantec SYM07-015 du 11 juillet 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 ;
- déni de service à distance.

2 Systèmes affectés

- *Backup Exec for Windows Servers* version 10 (build 10.0.5484) ;
- *Backup Exec for Windows Servers* version 10 (build 10.0.5520) ;
- *Backup Exec for Windows Servers* version 10d (build 10.1.5629) ;
- *Backup Exec for Windows Servers* version 11d (build 11.0.6235) ;
- *Backup Exec for Windows Servers* version 11d (build 11.0.7170).

3 Résumé

Une vulnérabilité dans l'interface RPC de *Backup Exec* permet de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire affecte l'interface `RPC` de *Backup Exec*. Un utilisateur malintentionné peut, par le biais d'un paquet `RPC` spécifiquement constitué à destination du port 6106/tcp du serveur *Backup Exec*, provoquer un déni de service ou exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Symantec SYM07-015 du 11 juillet 2007 :
<http://securityresponse.symantec.com/avcenter/security/Content/2007.07.11a.html>
- Référence CVE CVE-2007-3509 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3509>

Gestion détaillée du document

12 juillet 2007 version initiale.