

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Symantec Veritas 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-2006-AVI-353>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2006-AVI-353 |
| Titre | Vulnérabilité dans Symantec Veritas Backup Exec |
| Date de la première version | 11 août 2006 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Symantec #284623 du 31 juillet 2006 |
| 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 9.1 for Netware Servers Remote Agent for Windows Servers ;
- Backup Exec 9.2 for Netware Servers Remote Agent for Windows Servers.

3 Résumé

Une vulnérabilité dans l'application Backup Exec de Veritas permet à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité de type débordement de mémoire peut être exploitée par un individu malveillant au moyen d'un appel particulier adressé au service RPC (Remote Procedure Call). Une exploitation distante réalisée avec succès permet d'exécuter de code arbitraire ou de provoquer un déni de service.

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 #284623 du 31 juillet 2006 :
<http://seer.entsupport.symantec.com/docs/284623.htm>

Gestion détaillée du document

11 août 2006 version initiale.