

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de Symantec Veritas NetBackup

---

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-128>

---

### Gestion du document

Référence	CERTA-2006-AVI-128
Titre	Multiples vulnérabilités de Symantec Veritas NetBackup
Date de la première version	28 mars 2006
Date de la dernière version	–
Source(s)	Bulletin de Sécurité Symantec
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

Les versions Symantec NetBackup affectées sont :

- NetBackup Enterprise (client et serveur) 6.0
- NetBackup Enterprise (client et serveur) 5.1
- NetBackup Enterprise (client et serveur) 5.0
- NetBackup (client et serveur) 6.0
- NetBackup (client et serveur) 5.1
- NetBackup (client et serveur) 5.0
- NetBackup DataCenter et BusinesServer (client et serveur) 4.5FP
- NetBackup DataCenter et BusinesServer (client et serveur) 4.5MP

## 3 Résumé

Plusieurs vulnérabilités se trouvent dans les produits Veritas NetBackup. Celles-ci peuvent être utilisées par un utilisateur malveillant dans le but d'accéder à distance au système.

## 4 Description

Plusieurs vulnérabilités de type *débordement de mémoire* ont été trouvées dans l'ensemble des produits de stockage et d'archivage Veritas NetBackup. Elles concernent trois services communs à une grande majorité des produits, à savoir : `vmd`, `bpdbm` et `bpspsserver`. Un utilisateur malveillant peut envoyer des paquets utilisant ses vulnérabilités, afin de gagner accès au système.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité SYM06-006 :  
<http://seer.support.veritas.com/docs/281521.htm>
- Référence CVE CVE-2006-0989 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0989>
- Référence CVE CVE-2006-0990 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0990>
- Référence CVE CVE-2006-0991 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0991>

## Gestion détaillée du document

**28 mars 2006** version initiale.