

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-555>

Gestion du document

Référence	CERTA-2006-AVI-555
Titre	Vulnérabilités de Symantec Veritas NetBackup
Date de la première version	14 décembre 2006
Date de la dernière version	–
Source(s)	Avis de sécurité : SYM06-024
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

- NetBackup Entreprise Server/NetBackup Server ; client, serveur, et option *Storage Migrator* pour Unix : versions 6.0 antérieures à 6 . 0_MP4 ;
- NetBackup Entreprise Server/NetBackup Server ; client, serveur, et option *Storage Migrator* pour Unix : versions 5.1 antérieures à 5 . 1_MP6 ;
- NetBackup Entreprise Server/NetBackup Server ; client, serveur, et option *Storage Migrator* pour Unix : versions 5.0 antérieures à 5 . 0_MP7.

3 Description

NetBackup est un produit destiné à réaliser des sauvegardes et des restaurations.

Plusieurs vulnérabilités ont été identifiées. Elles affectent le *master*, les clients et les serveurs du logiciel *NetBackup*. Un individu malintentionné avec un accès à une machine disposant de la fonctionnalité *NetBackup* pourrait exécuter du code arbitraire pouvant résulter en une élévation de privilège.

Une première vulnérabilité due à un débordement de mémoire peut être exploitée sur le réseau par un individu malintentionné au moyen d'un paquet spécialement conçu.

Une deuxième vulnérabilité affecte le *daemon* `bpcc` qui traite l'exécution des commandes système. Le contrôle des commandes n'est pas fait correctement, et un individu malintentionné peut ajouter des commandes arbitraires à des commandes valides.

4 Contournement provisoire

Symantec recommande de ne jamais être exposé sur un réseau externe. La configuration devrait toujours restreindre les accès à des machines de confiance. Symantec recommande de mettre en place la fonctionnalité NBAC et de configurer l'accès réservé uniquement à des machines de confiance.

5 Solution

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

6 Documentation

- Référence CVE CVE-2006-4902 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4902>
- Référence CVE CVE-2006-5822 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5822>
- Référence CVE CVE-2006-6222 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6222>
- Avis de sécurité Symantec SYM06-024 :
<http://securityresponse.symantec.com/avcenter/security/Content/2006.12.13a.html>

Gestion détaillée du document

14 décembre 2006 version initiale.