

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de 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-2005-AVI-024>

---

### Gestion du document

Référence	CERTA-2005-AVI-024
Titre	Vulnérabilité de Veritas Backup Exec
Date de la première version	24 janvier 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité 273419 de Veritas
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

Veritas Backup Exec versions 8.6 et 9.x.

## 3 Description

Veritas Backup Exec est un serveur de sauvegarde.

Une vulnérabilité a été découverte dans la fonction de réception et de traitement des requêtes d'enregistrement. La requête d'enregistrement contient le nom de machine et le port du client qui veut se connecter. En donnant un nom de machine très long, un utilisateur mal intentionné qui se connecte sur le serveur Backup Exec peut exécuter du code arbitraire à distance avec les droits du service Backup Exec (généralement administrateur de domaine).

## 4 Contournement provisoire

Filtrer le port 6101/tcp au niveau des pare-feux.

## **5 Solution**

Appliquer le correctif (cf. section Documentation)

## **6 Documentation**

- Bulletin de sécurité 273419 de Veritas :  
<http://support.veritas.com/docs/273419>
- Correctif pour la version 8.60.3878 :  
<http://support.veritas.com/docs/273850>
- Correctif pour la version 9.0.4454 :  
<http://support.veritas.com/docs/274298>
- Correctif pour la version 9.1.4691 :  
<http://support.veritas.com/docs/273420>

## **Gestion détaillée du document**

**24 janvier 2005** version initiale.