

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-229>

Gestion du document

Référence	CERTA-2005-AVI-229
Titre	Multiples vulnérabilités de Veritas Backup Exec
Date de la première version	23 juin 2005
Date de la dernière version	–
Source(s)	Bulletins de sécurité Veritas VX05-001, VX05-002, VX05-003, VX05-005, VX05-006 et VX05-007 du 22 juin 2005
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 ;
- accès non autorisé au système avec les privilèges de l'administrateur ;
- élévation de privilèges ;
- déni de service.

2 Systèmes affectés

- Backup Exec 10.0 for Windows Servers rev. 5520 ;
- Backup Exec 10.0 for Windows Servers rev. 5484 ;
- Backup Exec 9.1 for Windows Servers rev. 4691 ;
- Backup Exec 9.0 for Windows Servers rev. 4454 ;
- Backup Exec 9.0 for Windows Servers rev. 4367 ;
- Backup Exec 9.1.307 for NetWare Servers ;
- Backup Exec 9.1.306 for NetWare Servers ;
- Backup Exec 9.1.1154 for NetWare Servers ;
- Backup Exec 9.1.1152.4 for NetWare Servers ;

- Backup Exec 9.1.1152 for NetWare Servers ;
- Backup Exec 9.1.1151.1 for NetWare Servers ;
- Backup Exec 9.1.1127.1 for NetWare Servers ;
- Backup Exec 9.1.1067.3 for NetWare Servers ;
- Backup Exec 9.1.1067.2 for NetWare Servers ;
- Backup Exec 9.0.4202 for NetWare Servers ;
- Backup Exec 9.0.4174 for NetWare Servers ;
- Backup Exec 9.0.4172 for NetWare Servers ;
- Backup Exec 9.0.4170 for NetWare Servers ;
- Backup Exec 9.0.4019 for NetWare Servers.

3 Résumé

De multiples vulnérabilités affectant Veritas Backup Exec permettent l'exécution de code arbitraire à distance ou l'obtention d'un accès avec les privilèges de l'administrateur.

4 Description

Veritas Backup Exec est un logiciel de sauvegarde.

Plusieurs vulnérabilités affectent ce produit :

- deux vulnérabilités de type débordement de mémoire dans Veritas Backup Exec Remote Agent permettent à un utilisateur mal intentionné de réaliser un déni de service par arrêt brutal du serveur ;
- une vulnérabilité de type débordement de mémoire dans Veritas Backup Exec Remote Agent for Windows Servers (RAWS) permet l'exécution de code arbitraire à distance sur le serveur ;
- une vulnérabilité dans la validation des accès distants permet l'obtention des privilèges de l'administrateur sur le registre du serveur ;
- une vulnérabilité de type débordement de mémoire dans Backup Exec Web Administration Console (BEWAC) permet l'exécution de code arbitraire à distance sur le serveur ;
- une vulnérabilité dans Admin Plus Pack Option permet à un utilisateur non autorisé d'obtenir un accès sur le serveur ;
- une vulnérabilité dans Veritas Backup Exec Remote Agent permet à un utilisateur d'élever ses privilèges.

5 Solution

Appliquer les correctifs indiqués dans le document 277429 de Veritas :
<http://seer.support.veritas.com/docs/277429.htm>

6 Documentation

- Bulletin de sécurité Veritas VX05-001 du 22 juin 2005 :
<http://seer.support.veritas.com/docs/276533.htm>
- Bulletin de sécurité Veritas VX05-002 du 22 juin 2005 :
<http://seer.support.veritas.com/docs/276604.htm>
- Bulletin de sécurité Veritas VX05-003 du 22 juin 2005 :
<http://seer.support.veritas.com/docs/276605.htm>
- Bulletin de sécurité Veritas VX05-005 du 22 juin 2005 :
<http://seer.support.veritas.com/docs/276606.htm>
- Bulletin de sécurité Veritas VX05-006 du 22 juin 2005 :
<http://seer.support.veritas.com/docs/276607.htm>
- Bulletin de sécurité Veritas VX05-007 du 22 juin 2005 :
<http://seer.support.veritas.com/docs/276608.htm>

Gestion détaillée du document

23 juin 2005 version initiale.