

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de VERITAS Cluster Server pour UNIX

---

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-448>

---

### Gestion du document

Référence	CERTA-2005-AVI-448
Titre	Vulnérabilité de VERITAS Cluster Server pour UNIX
Date de la première version	09 novembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM05-023 du 08 novembre 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

Elévation de privilèges.

## 2 Systèmes affectés

- VERITAS Storage Foundation Cluster File System 4.0 pour AIX, Linux et Solaris ;
- VERITAS SANPoint Control Quickstart 3.5 pour Solaris ;
- VERITAS Storage Foundation pour DB2 1.0 pour AIX, 4.0 pour AIX et Solaris ;
- VERITAS Storage Foundation pour Oracle 3.0 pour AIX, 3.5 pour Solaris, 4.0 pour Solaris et AIX ;
- VERITAS Storage Foundation pour Oracle Real Application Clusters 3.5 pour Solaris, 4.0 pour AIX, Linux et Solaris ;
- VERITAS Storage Foundation pour Sybase 4.0 pour Solaris ;
- VERITAS Storage Foundation pour UNIX 2.2 pour Linux et VMWare ESX, 3.4 pour AIX, 3.5 pour HP-UX et Solaris, 4.0 pour AIX, Linux et Solaris ;
- VERITAS Cluster Server 2.2 pour Linux (toutes versions), 3.5 pour Solaris, HP-UX, AIX (toutes versions), 4.0 pour Solaris, AIX, Linux (toutes versions).

### **3 Description**

Une vulnérabilité de type débordement de mémoire a été découverte dans VERTITAS Cluster Server, faisant partie de VERITAS Storage Foundation. Cette vulnérabilité correspond à une erreur dans la prise en compte de la variable d'environnement `VCS118N_LANG` par des commandes de type `ha`. L'exploitation de cette vulnérabilité permet à un utilisateur mal intentionné d'élever ses privilèges pour obtenir ceux du super-utilisateur `root`.

### **4 Solution**

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

### **5 Documentation**

- Bulletin de sécurité Symantec SYM05-023 du 08 novembre 2005 :  
<http://seer.support.veritas.com/docs/279870.htm>

### **Gestion détaillée du document**

**09 novembre 2005** version initiale.