

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Symantec Veritas Storage

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-2007-AVI-248>

Gestion du document

Référence	CERTA-2007-AVI-248
Titre	Vulnérabilités dans Symantec Veritas Storage
Date de la première version	04 juin 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité Symantec SYM07-009 du 01 juin 2007 Bulletins de sécurité Symantec SYM07-010 du 01 juin 2007
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Symantec Veritas Storage Foundation 5.x ;
- Symantec Veritas Storage Foundation 4.x ;
- Symantec Veritas Storage Foundation Cluster File System 4.x ;
- Symantec Veritas Storage Foundation for Database 4.x ;
- Symantec Veritas Storage Foundation for Oracle Real Application Clusters 4.x ;
- Symantec Veritas Volume Manager 3.x.

3 Résumé

Deux vulnérabilités découvertes dans les produits Symantec permettent à un utilisateur distant malintentionné de provoquer un déni de service, de contourner la politique de sécurité ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité dans le service `Scheduler Service` (`VxSchedService.exe`) peut être exploitée par un utilisateur malveillant pour contourner la politique de sécurité. Un individu peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire à distance.

Une seconde vulnérabilité dans le service `Veritas Volume Replicator` permet à une personne malintentionnée de provoquer l'arrêt brutal du service à distance ou, dans certaines circonstances, de consommer toutes les ressources du 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 Symantec SYM07-009 du 01 juin 2007 :
<http://securityresponse.symantec.com/avcenter/security/Content/2007.06.01.html>
- Bulletin de sécurité Symantec SYM07-010 du 01 juin 2007 :
<http://www.symantec.com/avcenter/security/Content/2007.06.01a.html>
- Référence CVE CVE-2007-1593 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1593>
- Référence CVE CVE-2007-2279 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2279>

Gestion détaillée du document

04 juin 2007 version initiale.