

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des produits Symantec Veritas VRTSweb

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-2009-AVI-542>

Gestion du document

Référence	CERTA-2009-AVI-542
Titre	Vulnérabilité des produits Symantec Veritas VRTSweb
Date de la première version	11 décembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM09-017 du 09 décembre 2009
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

- Symantec Backup Exec Continuous Protection Server (CPS) versions 11d, 12.0 et 12.5 ;
- Symantec Veritas NetBackup Operations Manager (NOM) versions 6.0 GA à 6.5.5 ;
- Symantec Veritas Backup Reporter (VBR) versions 6.0 GA à 6.6 ;
- Symantec Veritas Storage Foundation toutes versions ;
- Symantec Veritas Cluster Server toutes versions ;
- Symantec Veritas Application Director (VAD) versio 1.1 ;
- Symantec Veritas Command Central Storage (CCS) versions 4.x, 5.0 et 5.1 ;
- Symantec Veritas Command Central Enterprise Reporter (CC-ER) versions 5.0 GA, 5.0 MP1, 5.0 MP1RP1 et 5.1 ;
- Symantec Veritas Command Central Storage Change Manager (CC-SCM) versions 5.0 et 5.1 ;
- Symantec Veritas MicroMeasure version 5.0.

3 Résumé

Une vulnérabilité permettant l'exécution de code arbitraire à distance a été découverte dans les produits Symantec Veritas VRTSweb.

4 Description

Une vulnérabilité a été découverte dans les produits Symantec Veritas VRTSweb. Cette vulnérabilité est due à une mauvaise gestion du mécanisme d'authentification. L'exploitation de cette vulnérabilité permet à un utilisateur mal intentionné d'exécuter du code arbitraire depuis le réseau local.

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 SYM09-017 du 09 décembre 2009 :
<http://securityresponse.symantec.com/avcenter/security/Content/>
- Référence CVE CVE-2009-3027 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3027>

Gestion détaillée du document

11 décembre 2009 version initiale.