



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 28 février 2008
N° CERTA-2008-AVI-107

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Symantec Decomposer

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-2008-AVI-107>

Gestion du document

Référence	CERTA-2008-AVI-107
Titre	Vulnérabilités dans Symantec Decomposer
Date de la première version	28 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité SYM08-006 du 26 février 2008
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.

2 Systèmes affectés

- Symantec AntiVirus for Network Attached Storage versions 4.3.16.39 et antérieures ;
- Symantec AntiVirus Scan Engine versions 4.3.16.39 et antérieures ;
- Symantec Antivirus Scan Engine for Caching versions 4.3.16.39 et antérieures ;
- Symantec Antivirus Scan Engine for Clearswift versions 4.3.16.39 et antérieures ;
- Symantec Antivirus Scan Engine for Messaging versions 4.3.16.39 et antérieures ;
- Symantec Antivirus Scan Engine for MS ISA versions 4.3.16.39 et antérieures ;
- Symantec Antivirus Scan Engine for MS SharePoint versions 4.3.16.39 et antérieures ;
- toutes les versions de Symantec AntiVirus/Filtering for Domino MPE ;
- Symantec Mail Security for Microsoft Exchange versions 4.6.5.12 et antérieures ;
- Symantec Mail Security for Microsoft Exchange versions 5.0.4.363 et antérieures ;
- Symantec Scan Engine versions 5.1.4.24 et antérieures.

3 Résumé

Deux vulnérabilités dans le moteur *Symantec Decomposer* permettent de réaliser un déni de service et d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été découvertes dans le moteur *Symantec Decomposer* lors du traitement d'archives RAR. La première faille permet de réaliser un déni de service à distance par consommation excessive de la mémoire. La seconde, de type débordement de mémoire, permet l'exécution de code arbitraire à distance.

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 SYM08-006 du 26 février 2008 :
<http://securityresponse.symantec.com/avcenter/security/Content/2008.02.27.html>
- Référence CVE-2008-0308 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0308>
- Référence CVE-2008-0309 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0309>

Gestion détaillée du document

28 février 2008 version initiale.