

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités des produits Symantec

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-309>

Gestion du document

Référence	CERTA-2007-AVI-309
Titre	Multiples vulnérabilités des produits Symantec
Date de la première version	12 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec du 11 juillet 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 ;
- élévation de privilèges.

2 Systèmes affectés

- Symantec Gateway Security 5000 Series 3.x
- Symantec Gateway Security 5400 Series 2.x
- Symantec AntiVirus Corporate Edition 10.x
- Symantec AntiVirus Corporate Edition 9.x
- Symantec AntiVirus Corporate Edition for Linux
- Symantec AntiVirus for Macintosh 10.x
- Symantec AntiVirus for Network Attached Storage 4.x
- Symantec AntiVirus Scan Engine 4.x
- Symantec AntiVirus/Filtering for Domino 3.x
- Symantec Brightmail AntiSpam 4.x
- Symantec Brightmail AntiSpam 5.x

- Symantec Brightmail AntiSpam 6.x
- Symantec Client Security 2.x
- Symantec Client Security 3.x
- Symantec Mail Security for Domino 4.x
- Symantec Mail Security for Domino 5.x
- Symantec Mail Security for Exchange 4.x
- Symantec Mail Security for Microsoft Exchange 5.x
- Symantec Mail Security for Microsoft Exchange 6.x
- Symantec Mail Security for SMTP 5.x
- Symantec Norton AntiVirus 2004
- Symantec Norton AntiVirus 2005
- Symantec Norton AntiVirus 2006
- Symantec Norton AntiVirus for Macintosh 10.x
- Symantec Norton AntiVirus for Macintosh 9.x
- Symantec Norton Internet Security 2004
- Symantec Norton Internet Security 2004 Professional
- Symantec Norton Internet Security 2005
- Symantec Norton Internet Security 2006
- Symantec Norton Internet Security for Macintosh 3.x
- Symantec Norton Personal Firewall 2006
- Symantec Norton SystemWorks 2004
- Symantec Norton SystemWorks 2005
- Symantec Norton SystemWorks 2006
- Symantec Norton SystemWorks for Macintosh 3.x
- Symantec Scan Engine 5.x
- Symantec Web Security 3.x

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans de nombreux produits Symantec. L'exploitation de ces vulnérabilités permet d'effectuer un grand nombre d'actions malveillantes, dont le contrôle de la machine à distance.

4 Description

Plusieurs vulnérabilités ont été recensées dans les produits Symantec :

Module SYMTDI.SYS Cette vulnérabilité est due à une erreur dans la vérification de l'espace d'adressage dans SYMTDI.SYS. Cette vulnérabilité permet à un utilisateur local malintentionné d'exécuter du code tout en disposant des privilèges du noyau.

Scanneur en temps réel Cette vulnérabilité est due à une erreur dans le traitement des notifications par le scanneur en temps réel. Cette vulnérabilité permet à un utilisateur local malintentionné d'exécuter du code tout en disposant des privilèges SYSTEM.

Traitement des fichiers CAB et RAR Deux vulnérabilités ont été découvertes, respectivement dans le traitement des fichiers au format CAB et RAR. L'exploitation de ces vulnérabilités via un fichier spécialement conçu permet d'exécuter du code arbitraire à distance ou de réaliser un déni de service à distance.

5 Solution

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

6 Documentation

- Buletins de sécurité de Symantec du 11 juillet 2007 :
<http://securityresponse.symantec.com/avcenter/security/Content/20070711c.html>
<http://securityresponse.symantec.com/avcenter/security/Content/20070711d.html>
<http://securityresponse.symantec.com/avcenter/security/Content/20070711f.html>
- Références CVE :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3673>

Gestion détaillée du document

12 juillet 2007 version initiale.