

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les 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-2005-AVI-062>

Gestion du document

Référence	CERTA-2005-AVI-062
Titre	Vulnérabilités dans les produits Symantec
Date de la première version	10 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Symantec SYM05-003 du 08 février 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Norton AntiVirus pour Microsoft Exchange 2.1 versions antérieures à 2.18.85 ;
- Symantec Mail Security pour Microsoft Exchange 4.0 versions antérieures à 4.0.10.465 ;
- Symantec Mail Security pour Microsoft Exchange 4.5 versions antérieures à 4.5.3 ;
- Symantec AntiVirus/Filtering pour Domino NT 3.1 versions antérieures à 3.1.1 ;
- Symantec Mail Security pour Domino 4.0 versions antérieures à 4.0.1 ;
- Symantec AntiVirus/Filtering pour Domino Ports 3.0 (AIX) versions antérieures à 3.0.6 ;
- Symantec AntiVirus/Filtering pour Domino Ports 3.0 (OS400, Linux, Solaris) versions antérieures à 3.0.7 ;
- Symantec AntiVirus Scan Engine 4.3 versions antérieures à 4.3.3 ;
- Symantec AntiVirus pour Network Attached Storage versions antérieures à 4.3.3 ;
- Symantec AntiVirus pour Caching versions antérieures à 4.3.3 ;
- Symantec AntiVirus pour SMTP 3.1 versions antérieures à 3.1.7 ;
- Symantec Mail Security pour SMTP 4.0 versions antérieures à 4.0.2 ;
- Symantec Web Security 3.0 versions antérieures à 3.0.1.70 ;

- Symantec BrightMail AntiSpam 4.0 ;
- Symantec BrightMail AntiSpam 5.5 ;
- Symantec AntiVirus Corporate Edition 9.0 versions antérieures à 9.01.1000 ;
- Symantec AntiVirus Corporate Edition 8.01, 8.1.1 ;
- Symantec Client Security 2.0 versions antérieures à 9.01.1000 ;
- Symantec Client Security 1.0 ;
- Symantec Gateway Security 2.0, 2.0.1 - 5400 Series ;
- Symantec Gateway Security 1.0 - 5300 Series ;
- Symantec Norton Antivirus 2004 pour Windows ;
- Symantec Norton Internet Security 2004 (pro) pour Windows ;
- Symantec Norton System Works 2004 pour Windows ;
- Symantec Norton Antivirus 2004 pour Macintosh ;
- Symantec Norton Internet Security 2004 pour Macintosh ;
- Symantec Norton System Works 2004 pour Macintosh ;
- Symantec Norton Antivirus 9.0 pour Macintosh ;
- Symantec Norton Internet Security pour Macintosh 3.0 ;
- Symantec Norton System Works pour Macintosh 3.0.

3 Résumé

Une vulnérabilité présente dans divers produits Symantec lors du traitement des fichiers compressés avec UPX permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité a été découverte dans le moteur DEC2EXE qui est utilisé par les anciennes versions des produits Symantec pour le traitement des fichiers compressés avec UPX. Un utilisateur mal intentionné peut, par l'intermédiaire d'un fichier compressé UPX habilement constitué, exécuter du code arbitraire à distance.

Le moteur DEC2EXE n'est plus utilisé dans les versions récentes des produits Symantec.

5 Solution

Appliquer le correctif de Symantec, disponible depuis la page :
<http://www.symantec.com/techsupp>

6 Documentation

- Bulletin de sécurité Symantec SYM05-005 du 08 février 2005 :
<http://www.sarc.com/avcenter/security/Content/2005.02.08.html>

Gestion détaillée du document

10 février 2005 version initiale.