Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 avril 2006
N° CERTA-2006-AVI-166

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Symantec LiveUpdate pour Macintosh

Gestion du document

Référence	CERTA-2006-AVI-166
Titre	Vulnérabilité dans Symantec LiveUpdate pour Macintosh
Date de la première version	20 avril 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité de l'éditeur Symantec
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 ;
- élévation de privilèges.

2 Systèmes affectés

La plupart des outils Symantec utilisant LiveUpdate sous Macintosh sont affectés par cette vulnérabilité. Cela inclut :

- Symantec LiveUpdate pour Macintosh versions 3.0.X
- Symantec LiveUpdate pour Macintosh versions 3.5.X
- Norton AntiVirus 9.0.X
- Norton AntiVirus 10.X
- Symantec AntiVirus 10.X
- Norton Personal Firewall 3.0.X
- Norton Personal Firewall 3.1.0
- Norton Internet Security 3.0.X
- Norton Utilities 8.0.X
- Norton SystemWorks 3.0.X

3 Résumé

Une vulnérabilité présente dans certains modules de Symantec LiveUpdate pour le système d'exploitation Macintosh peut être utilisée par une personne malveillante pour élever ses droits sur la machine et exécuter des commandes arbitraires avec les droits dérobés.

4 Description

Une vulnérabilité existe dans certains modules de Symantec LiveUpdate pour le système d'exploitation Macintosh : ceux-ci ne définiraient pas correctement certaines variables d'environnement pour exécuter du code. Une personne malveillante peut donc lancer un de ces modules avec des variables d'environnement différentes, afin de profiter des droits d'administrateur pour exécuter du code arbitraire dans le 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 SYM06-007 du 17 avril 2006 :
http://securityresponse.symantec.com/avcenter/security/Content/2006.04.17b.html

Gestion détaillée du document

20 avril 2006 version initiale.