Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 décembre 2006
N° CERTA-2006-AVI-564

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de McAfee

Gestion du document

Référence	CERTA-2006-AVI-564
Titre	Vulnérabilité de McAfee
Date de la première version	19 décembre 2006
Date de la dernière version	–
Source(s)	Bulletin Gentoo 200612-15
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

McAfee Command Line Scanner pour Linux.

3 Résumé

McAfee Viruscan est un logiciel antivirus qui peut être exécuté en ligne de commande. Une mauvaise gestion des répertoires permet à un utilisateur malintentionné d'élever ses privilèges et d'exécuter du code arbitraire.

4 Description

Le répertoire courant est inclus dans la liste des répertoires parcourus lors de la recherche les librairies utilisées pour l'analyse antivirale. Un utilisateur malveillantattaquant peut créer un objet malveillant dans un répertoire et

inciter à utiliser *McAfee Command Line Scanner* depuis ce répertoire. L'attaquant fera exécuter le code malveillant avec les privilèges du logiciel antivirus.

Il convient de n'exécuter l'analyser en ligne de commande que depuis un répertoire sûr.

La version pour Windows n'est pas concernée.

5 Solution

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

6 Documentation

- Bulletin de sécurité Gentoo GLSA-200612-15 du 14 décembre 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200612-15.xml
- Référence CVE CVE-2006-6474 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6474

Gestion détaillée du document

19 décembre 2006 version initiale.