



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 21 mars 2005  
N° CERTA-2005-AVI-118

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans les produits McAfee

---

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-118>

---

### Gestion du document

Référence	CERTA-2005-AVI-118
Titre	Vulnérabilité dans les produits McAfee
Date de la première version	21 mars 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité McAfee
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

- Déni de service ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

Les produits McAfee suivant ayant une version du moteur d'analyse antérieure à la version 4.4.00.

- Active Virus Defense ;
- Active VirusScan ;
- Active Virus Defense SMB Edition ;
- Active VirusScan SMB Edition ;
- Active Threat Protection ;
- Active Mail Protection ;
- GroupShield pour Exchange ;
- GroupShield pour Exchange 5.5 ;
- GroupShield pour Lotus Domino ;
- GroupShield pour Mail Servers with ePO ;
- LinuxShield ;

- NetShield pour Netware ;
- PortalShield pour Microsoft SharePoint ;
- SecurityShield pour Microsoft ISA Server ;
- Virex ;
- VirusScan (toutes versions) ;
- VirusScan Professional ;
- VirusScan ASaP/Managed VirusScan ;
- VirusScan Command Line ;
- VirusScan pour NetApp ;
- VirusScan(r) Enterprise(toutes versions) ;
- WebShield Appliances ;
- WebShield SMTP.

### **3 Résumé**

Une vulnérabilité présente dans les moteurs d'analyse des produits McAfee peut être exploitée par un utilisateur mal intentionné pour réaliser un déni de service ou exécuter du code arbitraire.

### **4 Description**

Un débordement de mémoire est présent sur les moteurs d'analyse des produits McAfee. Un utilisateur mal intentionné peut exploiter cette vulnérabilité, via l'utilisation de fichier LHA malicieusement construit, pour réaliser un déni de service ou exécuter du code arbitraire sur le système.

### **5 Solution**

Pour l'obtention des correctifs consulter le bulletin de sécurité de l'éditeur (cf. section Documentation).

### **6 Documentation**

- Site internet McAfee :  
<http://www.mcafee.fr>
- Bulletin de sécurité McAfee :  
<http://ts.mcafeehelp.com/faq3.asp?docid=378097>

### **Gestion détaillée du document**

**21 mars 2005** version initiale.