

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans McAfee WebShield SMTP

---

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-2006-AVI-135>

---

### Gestion du document

Référence	CERTA-2006-AVI-135
Titre	Vulnérabilité dans McAfee WebShield SMTP
Date de la première version	04 avril 2006
Date de la dernière version	–
Source(s)	
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

Pour l'instant, la vulnérabilité porte sur la version 4.5 MR1a pour les systèmes Windows.

## 3 Description

Cette vulnérabilité sur l'application McAfee WebShield SMTP, peut être exploitée afin de compromettre la machine vulnérable et d'y exécuter du code arbitraire à distance. Cette vulnérabilité est liée au format des chaînes de caractères pour les messages d'erreur dans le cadre des messages retournés ("bounce messages"). Ce type de message d'erreur est appelé DSN, "Delivery Status Notification" (note du CERTA sur le spam, cf. section Documentation). Un "bounce message" est un message retourné à l'expéditeur indiquant que l'adresse du destinataire n'a pas été trouvée. Dans le cas présent, la vulnérabilité exploite les "bounce messages" indiquant des domaines qui n'existent pas.

## **4 Solution**

Se référer au bulletin de sécurité de l'éditeur qui recommande l'installation de la version 4.5 MR2 de l'application (cf. section Documentation).

## **5 Documentation**

- Site de McAfee :  
<http://www.mcafee.com/fr/support/default.asp>
- Référence CVE CAN-2006-0559 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0559>
- Note du CERTA sur le SPAM :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004/index.html>

## **Gestion détaillée du document**

**04 avril 2006** version initiale.