Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 novembre 2009
N° CERTA-2009-AVI-497

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans McAfee IntruShield Network Security Manager

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-2009-AVI-497

Gestion du document

Référence	CERTA-2009-AVI-497
Titre	Vulnérabilités dans McAfee Network Security Manager
Date de la première version	12 novembre 2009
Date de la dernière version	–
Sources	Bulletins de sécurité McAfee SB10004 et SB10005 du 06 novembre 2009
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

- Contournement de la politique de sécurité ;
- injection de code indirecte.

2 Systèmes affectés

McAfee IntruShield NSM 5.1.x.

3 Résumé

Deux vulnérabilités dans *McAfee IntruShield NSM* (Network Security Manager) permettent à un utilisateur malveillant de réaliser du vol de session ou de l'injection de code indirecte.

4 Description

Une première vulnérabilité provient de la création du *cookie* d'authentification utilisé par *McAfee IntruShield NSM*. Elle est exploitable par un utilisateur malveillant pour voler une session.

Une deuxième vulnérabilité réside dans le manque de validation des entrées par la console d'administration de *McAfee IntruShield NSM*. Elle est exploitable par un utilisateur malveillant pour réaliser de l'injection de code indirecte à l'encontre des administrateurs.

5 Solution

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

6 Documentation

- Bulletins de sécurité McAfee SB10004 et SB10005 du 06 novembre 2009 :
  https://kc.mcafee.com/corporate/index?page=content&id=SB10004
  https://kc.mcafee.com/corporate/index?page=content&id=SB10005
- Référence CVE CVE-2009-3565 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3565
- Référence CVE CVE-2009-3566 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3566

Gestion détaillée du document

12 novembre 2009 version initiale.