Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 mars 2012
N° CERTA-2012-AVI-143

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans McAfee EWS et MEG

Gestion du document

Référence	CERTA-2012-AVI-143
Titre	Multiples vulnérabilités dans McAfee EWS et MEG
Date de la première version	15 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité McAfee SB10020 du 13 mars 2012
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 ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

- McAfee Email and Web Security 5.5 et 5.6 ;
- McAfee Email Gateway 7.0.

3 Résumé

De multiples vulnérabilités ont été corrigées dans McAfee Email and Web Security et McAfee Email Gateway, qui permettent une injection de code indirecte à distance, de contourner la politique de sécurité, et de lire des données non autorisées.

4 Description

De multiples vulnérabilités ont été corrigées dans McAfee Email and Web Security et McAfee Email Gateway :

- une injection de code indirecte à distance, qui peut être exploitée par un attaquant pour acquérir des jetons de connexion et exécuter du code javascript dans le contexte de l'application client d'un administrateur ;
- la fermeture de la session ne se fait pas correctement et un attaquant peut exploiter cette vulnérabilité pour se connecter avec l'identité de l'utilisateur ;
- un utilisateur peut réinitialiser les mots de passe des administrateurs ;
- les jetons de sessions actives sont dévoilés dans le tableau de bord ;
- il est possible de retrouver les mots de passe dans les sauvegardes du système ;
- n'importe quel utilisateur distant peut lire des fichiers arbitraires du serveur ;
- n'importe quel utilisateur distant accède aux fichiers comme s'il était administrateur.

5 Solution

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

6 Documentation

- Bulletin de sécurité McAfee SB10020 du 13 mars 2012 :
  https://kc.mcafee.com/corporate/index?page=content&id=SB10020

Gestion détaillée du document

15 mars 2012 version initiale.