Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mars 2003
N° CERTA-2003-AVI-062

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Faille dans McAfee "Security ePolicy Orchestrator"

Gestion du document

Référence	CERTA-2003-AVI-062
Titre	Faille dans McAfee "Security ePolicy Orchestrator"
Date de la première version	26 mars 2003
Date de la dernière version	–
Source(s)	Avis de sécurité @stake du 17/03/2003
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire à distance avec des privilèges élevés.

2 Systèmes affectés

Tout système Microsoft Windows dont le service "Agent NAI ePolicy Orchestrator" est démarré.

3 Résumé

Une vulnérabilité de type chaîne de format, permet à un utilisateur mal intentionné distant d'exécuter du code sur la machine visée avec les privilèges élevés du niveau *SYSTEM*.

4 Description

"ePolicy Orchestrator" est un outil de gestion centralisée de la politique de sécurité antivirale. Il est composé de consoles d'administration, de serveurs et enfin d'agents sur chaque poste où la politique antivirus doit être appliquée et surveillée.

Les agents sont des services ayant les privilèges *SYSTEM* qui peuvent être interrogés à l'aide du protocole *HTTP* sur le port 8081/tcp. Une mauvaise gestion des chaînes de format dans ces requêtes permet l'exécution de code arbitraire.

5 Contournement provisoire

Afin de prévenir toute agression externe, les pare-feux peuvent être configurés pour filtrer le port 8081/tcp, cependant la faille reste alors exploitable depuis la même zone de sécurité. Si un pare-feu personnel est présent sur l'hôte, il peut être paramètré pour restreindre au serveur "ePolicy Orchestrator" les adresses IP autorisées à se connecter au port 8081/tcp.

6 Solution

Contacter votre revendeur NAI pour obtenir le correctif.

7 Documentation

- Description du produit "ePolicy Orchestrator" :
  http://www.mcafeeb2b.com/international/france/products/epolicy/default-management-solution.asp
- Avis de sécurité de @stake :
  http://www.atstake.com/research/advisories/2003/a031703-1.txt
- Référence CVE CAN-2002-0690 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0690

Gestion détaillée du document

26 mars 2003 version initiale.