Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 août 2003
N° CERTA-2003-AVI-133

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples failles dans McAfee «Security ePolicy Orchestrator»

Gestion du document

Référence	CERTA-2003-AVI-133
Titre	Multiples failles dans McAfee »Security ePolicy Orchestrator»
Date de la première version	1er août 2003
Date de la dernière version	–
Source(s)	Avis de sécurité @stake du 31/07/2003
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 ;
- divulgation d'informations.

2 Systèmes affectés

Tout système Microsoft Windows dont les services «NAI ePolicy Orchestrator» en version serveur ou agent sont démarrés.

3 Résumé

Des vulnérabilités permettent à un utilisateur mal intentionné distant d'exécuter du code sur une machine hébergeant un agent ou un serveur avec les privilèges élevés du niveau *SYSTEM*. De plus, l'ensemble des fichiers de l'hôte d'un agent en version 3.0 est accessible en lecture.

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.

Trois vulnérabilités permettant l'exécution de code arbitraire avec les privilèges *SYSTEM* ont été découvertes :

- sur les serveurs en version 2.x et 3.0 il est possible d'obtenir, à l'aide d'une requête HTTP bien formée, la configuration du serveur. On y trouve entre autres le compte utilisé et son mot de passe chiffré. L'algorithme de chiffrement et la clef utilisée pouvant être retrouvés, il est possible de faire exécuter sur l'hôte des commandes arbitraires en s'authentifiant sous ce compte.
- Une mauvaise gestion des chaînes de format dans les serveurs en version 2.x permet d'exécuter du code avec les privilèges du service à l'aide d'une requête HTTP POST.
- Inversement une commande POST habilement constituée et envoyée à un client provoque un débordement de mémoire et permet l'exécution de code.

Enfin une requête HTTP bien construite envoyée à un agent permet de lire n'importe quel fichier du système hôte.

5 Solution

Contacter votre revendeur NAI pour obtenir le correctif :
http://www.networkassociates.com/us/downloads/updates/hotfixes.asp

6 Documentation

- Description du produit «ePolicy Orchestrator» :
  http://www.mcafeesecurity.com/international/france/products/epolicy/default-management-solution.asp
- Avis de sécurité et correctif de NAI :
  http://www.nai.com/us/promos/mcafee/epo_vulnerabilities.asp
- Avis de sécurité de @stake :
  http://www.atstake.com/research/advisories/2003/a073103-1.txt
- Référence CVE CAN-2003-0148 «ePO MSDE SA account compromise» :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0148
- Référence CVE CAN-2003-0149 «ePO 2.x Post Parameters Heap Overflow» :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0149
- Référence CVE CAN-2003-0616 «ePO 2.x Compuerlist format string» :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0616
- Référence CVE CAN-2003-0610 «ePO 3.0 Agent Directory Traversal» :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0610

Gestion détaillée du document

1er août 2003 version initiale.