Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 mai 2007
N° CERTA-2007-AVI-185-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Apple MacOS X

Gestion du document

Référence	CERTA-2007-AVI-185-001
Titre	Multiples vulnérabilités dans Apple MacOS X
Date de la première version	20 avril 2007
Date de la dernière version	03 mai 2007
Source(s)	Bulletin de mise à jour Apple
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 ;
- déni de service à distance ;
- déni de service ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- *Apple MacOS X* version 10.3.x et 10.4.x ;
- *Apple MacOS X server* version 10.3.x et 10.4.x.

3 Résumé

Plusieurs vulnérabilités sous *Apple MacOS X* permettent à un utilisateur malveillant de compromettre un système vulnérable, localement ou à distance.

4 Description

Plusieurs vulnérabilités sont présentes sous *Apple MacOS X* :

- une vulnérabilité du client *AFP* permet à un utilisateur local de créer des fichiers ou d'exécuter des commandes avec les privilèges système ;
- une vulnérabilité dans *Airport* de type débordement de mémoire permettrait l'exécution d'un code arbitraire avec des privilèges élevés ;
- une vulnérabilité de *CarbonCore* permet l'exécution d'un code arbitraire avec des privilèges élevés ;
- une vulnérabilité dans `fsck` permet à un utilisateur d'exécuter du code arbitraire à distance en incitant un utilisateur à charger un fichier image (`.dmg`) spécialement conçu;
- une vulnérabilité dans *fetchmail* provoque l'envoi d'informations d'authentification en clair, même lorsque la configuration exige l'utilisation de TLS ;
- un débordement de mémoire dans *ftpd* permet à un utilisateur authentifié d'exécuter un code arbitraire à distance ;
- une mauvaise gestion de format dans *Help Viewer* et un débordement de mémoire dans *GNU Tar* permettent à un utilisateur malintentionné de provoquer un arrêt inopiné de l'application ou d'exécuter du code arbitraire ;
- un contrôle insuffisant dans *HID* permet à un utilisateur malveillant de capturer les entrées au clavier, y compris les données sensibles ;
- une erreur de gestion de format dans *Installer* permet à un utilisateur malintentionné de provoquer un arrêt inopiné de l'application ou d'exécuter du code arbitraire à distance ;
- une erreur dans *WebFoundation* permet à un domaine parent de lire un *cookie* positionné par l'un de ses sous-domaines ;
- le défaut de gestion de l'environnement par *WebDav* permet à un utilisateur local malintentionné de créer des fichiers ou d'exécuter des commandes avec les privilèges système ;
- un défaut de validation des paquets SIP par *Videoconference* permet à un utilisateur malintentionné d'exécuter un code arbitraire à distance ;
- *URLMount* monte des systèmes de fichiers distants via un serveur SMB en appelant la commande `mount_smb` ; Les identifiants et les mots de passe sont transmis comme arguments en ligne de commande, ce qui les expose à être divulgués à d'autres utilisateurs ;
- un manque de contrôle dans `launchctl` permet aux administrateurs locaux de lancer des commandes avec les privilèges système sans s'authentifier ;
- le défaut de gestion de l'environnement par le serveur SMB permettrait à un utilisateur local malintentionné de créer des fichiers ou d'exécuter des commandes avec les privilèges système ;
- lorsque le partage *Internet Sharing* est actif, un mauvais traitement de paquets RTSP permet à un utilisateur mal intentionné de provoquer un déni de service ou l'exécution de code arbitraire à distance ;
- des erreurs dans *Login Window* permettent à un utilisateur local de se connecter sans authentification ou d'élever ses privilèges ;
- des erreurs dans *Libinfo* permettent à un utilisateur malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire à distance ;
- des vulnérabilités dans le démon d'administration de *Kerberos* permettent à un utilisateur malintentionné de provoquer un arrêt inopiné de l'application ou l'exécution de code arbitraire avec les droits système.

Apple a publié le 01 mai 2007 deux mises à jour de correctifs. La première concerne les pilotes sans-fil Airport pour Mac OS X v10.3.9, et la seconde le serveur FTP `FTPServer` sous Mac OS X v10.4.9. Le précédent correctif applique un fichier de configuration FTP incorrect, qui permettrait aux utilisateurs d'accéder illégitimement à certains répertoires.

5 Solution

Appliquer la mise à jour de sécurité 2007-004., ainsi que le correctif de cette mise à jour (v1.1). Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple du 19 avril 2007 :
  http://docs.info.apple.com/article.html?artnum=305391

- Mise à jour du bulletin précédent, faite le 01 mai 2007 : http://docs.info.apple.com/article.html?artnum=305445
- Référence CVE CVE-2007-0745 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0745
- Référence CVE CVE-2006-0300 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0300
- Référence CVE CVE-2006-5867 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5867
- Référence CVE CVE-2006-6143 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6143
- Référence CVE CVE-2006-6652 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6652
- Référence CVE CVE-2007-0022 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0022
- Référence CVE CVE-2007-0465 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0465
- Référence CVE CVE-2007-0646 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0646
- Référence CVE CVE-2007-0724 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0724
- Référence CVE CVE-2007-0725 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0725
- Référence CVE CVE-2007-0729 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0729
- Référence CVE CVE-2007-0732 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0732
- Référence CVE CVE-2007-0734 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0734
- Référence CVE CVE-2007-0735 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0735
- Référence CVE CVE-2007-0736 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0736
- Référence CVE CVE-2007-0737 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0737
- Référence CVE CVE-2007-0738 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0738
- Référence CVE CVE-2007-0739 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0739
- Référence CVE CVE-2007-0741 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0741
- Référence CVE CVE-2007-0742 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0742
- Référence CVE CVE-2007-0743 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0743
- Référence CVE CVE-2007-0744 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0744
- Référence CVE CVE-2007-0746 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0746
- Référence CVE CVE-2007-0747 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0747
- Référence CVE CVE-2007-0927 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0957

- Référence CVE CVE-2007-0957 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0957
- Référence CVE CVE-2007-1216 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1216

Gestion détaillée du document

20 avril 2007 version initiale.
03 mai 2007 ajout de la mise à jour du bulletin d'avril 2007, ainsi que la référence au CVE CVE-2007-0745.