Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mai 2007
N° CERTA-2007-AVI-234

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Apple Mac OS X

Gestion du document

Référence	CERTA-2007-AVI-234
Titre	Multiples vulnérabilités dans Apple Mac OS X
Date de la première version	30 mai 2007
Date de la dernière version	–
Source(s)	Avis de sécurité Apple 2007-005 305530 du 29 mai 2007
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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Apple Mac OS X v10.3.9 ;
- Apple Mac OS X Server v10.3.9 ;
- Apple Mac OS X v10.4.9 ;
- Apple Mac OS X Server v10.4.9.

3 Résumé

Plusieurs vulnérabilités ont été identifiées : elles concernent le système d'exploitation Mac OS X. L'exploitation de ces dernières peut avoir des conséquences variées, comme l'exécution de code arbitraire, ou un dysfonctionnement du système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le système d'exploitation Mac OS X. Parmi celles-ci :

- `Alias Manager` : il existerait, sous certaines conditions, une incohérence sur les noms de fichier lorsque deux images disque sont montées. Cette vulnérabilité pourrait être exploitée pour faire ouvrir et/ou exécuter un fichier différent de celui demandé sur le système vulnérable ;
- `BIND` : plusieurs vulnérabilités ont été corrigées dans le serveur `DNS` pour Mac OS X. Elles sont semblables à celles décrites dans les avis CERTA-2006-AVI-385 et CERTA-2007-AVI-056 ;
- `CoreGraphics` : l'application ne manipulerait pas correctement certains fichiers au format `PDF` (pour *Portable Document Format*), pouvant entraîner l'exécution de commande arbitraire à distance ;
- `crontabs` : le gestionnaire de tâches pourrait perturber le système de fichiers monté dans le répertoire `/tmp`, par le biais du script de nettoyage journalier.
- `fetchmail` : une vulnérabilité présente dans `fetchmail` permettrait de récupérer tout ou partie d'un mot de passe échangé au cours de l'initialisation de la connexion POP3. Cette vulnérabilité est différente de celle décrite dans CERTA-2007-AVI-020.
- `file` : la commande `file` ne manipule pas correctement certains fichiers, ce qui peut provoquer l'interruption de la commande, voire l'exécution de code arbitraire sur le système vulnérable.
- `iChat` : l'application de messagerie instantanée ne gère pas correctement certains paquets `UPnP IGD` (pour *Internet Gateway Device Standardized Device Control Protocol*). Une personne malveillante distante peut ainsi exploiter cette vulnérabilité en envoyant un paquet spécialement construit, afin de perturber l'application ou d'exécuter du code arbitraire à distance.
- `mDNSResponder` : le problème est identique à celui présenté pour `iChat` mais n'affecterait que les versions au moins équivalentes à Mac OS X v10.4 ;
- `PPP` : le démon `PPP` ne chargerait pas correctement certains modules au cours de son lancement en ligne de commandes, ce qui permettrait à une personne malveillante locale d'élever ses privilèges sur le système vulnérable ;
- `ruby` : les vulnérabilités corrigées ont été présentées dans l'avis CERTA-2006-AVI-562 ;
- `screen` : le service `GNU Screen` auraient plusieurs vulnérabilités exploitables par la ligne de commande `screen`, et qui provoqueraient sous certaines conditions un déni de service.
- `texinfo` : une vulnérabilité permettrait d'élever ses privilèges à ceux de l'utilisateur utilisant `texinfo` afin de créer ou d'écraser des fichiers d'accès limité.
- `VPN` : le démon `vpnd` ne manipulerait pas correctement certaines chaînes de caractères, permettant à un utilisateur local d'élever ses privilèges à ceux du système et d'exécuter du code arbitraire sur la machine.

5 Solution

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

6 Documentation

- Bulletin de sécurité Apple du 29 mai 2007 :
  http://docs.info.apple.com/article.html?artnum=305530
- Référence CVE CVE-2005-3011 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3011
- Référence CVE CVE-2006-4095 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4095
- Référence CVE CVE-2006-4096 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4096
- Référence CVE CVE-2007-4573 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4573
- Référence CVE CVE-2006-5467 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5467
- Référence CVE CVE-2006-6303 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6303

- Référence CVE CVE-2007-0493 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0493
- Référence CVE CVE-2007-0494 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0494
- Référence CVE CVE-2007-0740 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0740
- Référence CVE CVE-2007-0750 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0750
- Référence CVE CVE-2007-0751 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0751
- Référence CVE CVE-2007-0752 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0752
- Référence CVE CVE-2007-0753 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0753
- Référence CVE CVE-2007-1536 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1536
- Référence CVE CVE-2007-1558 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1558
- Référence CVE CVE-2007-2386 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2386
- Référence CVE CVE-2007-2390 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2390
- Avis de sécurité Fetchmail associé SA-2007-01 du 18 mars 2007 :
  http://fetchmail.berlios.de/fetchmail-SA-2007-01.txt
- Message dans la liste de diffusion GNU concernant GNU Screen paru en octobre 2006 :
  http://lists.gnu.org/archive/html/screen-users/2006-10/msg00028.html

Gestion détaillée du document

30 mai 2007 version initiale.