Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 octobre 2004
N° CERTA-2004-AVI-331

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Mac OS X

Gestion du document

Référence	CERTA-2004-AVI-331
Titre	Multiples vulnérabilités dans Mac OS X
Date de la première version	07 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité d'Apple du 30 septembre 2004
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

- Déni de service ;
- exécution de code arbitraire à distance ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

- Apple Mac OS X v10.3.5 ;
- Apple Mac OS X Server v10.3.5 ;
- Apple Mac OS X v10.2.8 ;
- Apple Mac OS X Server v10.2.8.

3 Résumé

De multiples vulnérabilités présentes dans le système d'exploitation Mac OS X d'Apple peuvent être exploitées par un utilisateur mal intentionné afin de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

L'intégrité et la confidentialité des données présentes sur le système vulnérable peuvent être affectées.

4 Description

- Le service AFP est un protocole d'Apple qui permet le partage de fichiers :
  - Une vulnérabilité présente dans ce service permet à un utilisateur connecté en tant qu'invité d'y réaliser un déni de service. (CVE CAN-2004-0921)
  - Une seconde vulnérabilité dans le service AFP permet à un utilisateur connecté en tant qu'invité de porter atteinte à l'intégrité des données du système dûe à une gestion incorrecte des groupes. (CVE CAN-2004-0922)
- Le service CUPS (Common Unix Printing System) met en œuvre un protocole Internet d'impression (IPP) :
  - Une vulnérabilité présente dans ce service permet à une personne malveillante de réaliser un déni de service au moyen d'un paquet UDP malicieusement constitué à destination du port IPP (CVE CAN-2004-0558).
  - Une seconde vulnérabilité dans le module d'impression à distance authentifié permet à une personne de porter atteinte à la confidentialité des données du système, en révélant les mots de passe contenus dans le journal des événements du système d'impression. (CVE CAN-2004-0923)
- L'application NetInfoManager permet de surveiller l'activité des fichiers partagés :
  Une vulnérabilité présente dans l'application NetInfoManager permet à un utilisateur de porter atteinte à l'intégrité des données du système vulnérable. En exploitant cette vulnérabilité, une personne malveillante peut activer le compte `root` qu'il est ensuite impossible de désactiver au moyen de NetInfoManager. (CVE CAN-2004-0924)
- L'application Postfix permet le transport de courrier électronique :
  Une vulnérabilité présente dans Postfix lorsque le protocole `SMTPD-AUTH` est activé, permet à un utilisateur mal intentionné de réaliser un déni de service. (CVE CAN-2004-0925)
- Le lecteur multimédia Quicktime présente une vulnérabilité de type débordement de mémoire (`buffer overflow`) lors du décodage d'une image `.bmp`. Une personne malveillante peut ainsi exécuter un code arbitraire sur la machine vulnérable grâce à un fichier `.bmp` malicieusement constitué. (CVE CAN-2004-0926)
- Le service Server Admin offre une interface graphique à l'utilisateur pour configurer et surveiller le réseau et les services Internet :
  une vulnérabilité découverte dans ce service permet à une personne mal intentionnnée de porter atteinte à la confidentialité des données. Server Admin dialogue avec le service Server Communication au moyen du protocole SSL, en utilisant des certificats fournis à titre d'exemple lors de l'installation par défaut des systèmes. (CVE CAN-2004-0927)

5 Solution

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

6 Documentation

- Bulletin de sécurité d'Apple du 30 septembre 2004 :
  `http://docs.info.apple.com/article.html?artnum=61798`
- Référence CVE CAN-2004-0558 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0558`
- Référence CVE CAN-2004-0921 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0921`
- Référence CVE CAN-2004-0922 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0922`
- Référence CVE CAN-2004-0923 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0923`
- Référence CVE CAN-2004-0924 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0924`
- Référence CVE CAN-2004-0925 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0925`

- Référence CVE CAN-2004-0926 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0926`
- Référence CVE CAN-2004-0927 :
  `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0927`

Gestion détaillée du document

07 octobre 2004 version initiale.