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 décembre 2004
N° CERTA-2004-AVI-386

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Mac OS X

Gestion du document

Référence	CERTA-2004-AVI-386
Titre	Multiples vulnérabilités dans Mac OS X
Date de la première version	03 décembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité d'Apple du 02 décembre 2004
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

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

1 Risque

- Elévation de privilèges ;
- déni de service ;
- exécution de code arbitraire ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Apple Mac OS X v10.3.6 ;
- Apple Mac OS X v10.2.8 ;
- Apple Mac OS X Server v10.3.6 ;
- Apple Mac OS X Server v10.2.8 ;

3 Résumé

De multiples vulnérabilités découvertes 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, d'exécuter du code arbitraire, d'élever ses privilèges ou de porter atteinte à l'intégrité des données.

4 Description

- De multiples vulnérabilités dans le serveur web Apache permet à un utilisateur malveillant d'élever localement ses privilèges, d'effectuer un déni de service à distance et d' exécuter du code arbitraire sur le serveur vulnérable (cf. références CAN-2004-1082, CAN-2003-0020, CAN-2003-0987, CAN-2004-0174, CAN-2004-0488, CAN-2004-0492, CAN-2004-0885, CAN-2004-0940, CAN-2004-1083, CAN-2004-1084 et bulletin de sécurité CERTA-2004-AVI-370 du CERTA) ;
- une vulnérabilité est présente dans Apache 2 permettant à un individu mal intentionné d'effectuer un déni de service à distance ou d'élever ses privilèges sur le serveur affecté (cf. références CAN-2004-0747, CAN-2004-0786, CAN-2004-0751, CAN-2004-0748 et bulletin de sécurité CERTA-2004-AVI-313 du CERTA) ;
- Deux vulnérabilités présentes dans Appkit permettent à une personne malveillante d'exécuter du code arbitraire, d'effectuer un déni de service ou de porter atteinte à la confidentialité des données (cf. références CAN-2004-1081, CAN-2004-0803, CAN-2004-0804 et CAN-2004-0886) ;
- une vulnérabilité découverte dans Cyrus IMAP permet à un utilisateur mal intentionné de porter atteinte à la confidentialité des données portant sur les boîtes de messagerie électroniques présentes sur le système (cf. références CAN-2004-1089 et bulletin de sécurité CERTA-2004-AVI-379 du CERTA) ;
- une vulnérabilité dans HIToolbox permet à un utlisateur mal intentionné de forcer la fermeture de l'application au moyen d'une combinaison de touche spéciale (cf. référence CAN-2004-1085) ;
- une vulnérabilité dans le protocole d'authentification Kerberos permet à une personne malveillante d'effectuer un déni de service (cf. références CAN-2004-0642, CAN-2004-0643, CAN-2004-0644, CAN-2004-0772 et bulletin de sécurité CERTA-2004-AVI-362 du CERTA) ;
- une vulnérabilité découverte dans Postfix permet à un individu mal intentionné d'envoyer des messages électronique sans avoir été correctement authentifié par un serveur Postfix utilisant CRAM-MD5 (cf. référence CAN-2004-1088) ;
- une vulnérabilité de type débordement de mémoire est présente dans PSNormalizer. Lors d'une conversion de document PostScript en PDF (Portable Document Format). Cette vulnérabilité permet à une personne malveillante d'exécuter du code arbitraire à distance (cf. référence CAN-2004-1086) ;
- une vulnérabilité présente dans le serveur de flux QuickTime permet à un utilisateur mal intentionné d'effectuer un déni de service au moyen de requêtes malicieusement constituées (cf. référence CAN-2004-1123) ;
- Deux vulnérabilités découvertes dans le navigateur Internet Safari permettent à une personne malveillante d'afficher de fausses informations dans Safari, notamment au moyen d'une page HTML malicieusement constituée (cf. références CAN-2004-1121 et CAN-2004-1122) ;
- une vulnérabilité dans Terminal affiche à l'utilisateur que l'option 'Secure Keyboard Entry' est activée alors qu'elle ne l'est pas (cf. référence CAN-2004-1087).

5 Solution

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

6 Documentation

- Bulletin de sécurité d'Apple du 02 décembre 2004
  http://docs.info.apple.com/article.html?artnum=61798
- Bulletin de sécurité CERTA-2004-AVI-370 du CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-370/
- Bulletin de sécurité CERTA-2004-AVI-313 du CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-313/
- Bulletin de sécurité CERTA-2004-AVI-379 du CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-379/
- Bulletin de sécurité CERTA-2004-AVI-362 du CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-362/
- Référence CVE CAN-2004-1082 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1082

- Référence CVE CAN-2003-0020 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0020
- Référence CVE CAN-2003-0987 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0987
- Référence CVE CAN-2004-0174 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0174
- Référence CVE CAN-2004-0488 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0488
- Référence CVE CAN-2004-0492 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0492
- Référence CVE CAN-2004-0885 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0885
- Référence CVE CAN-2004-0940 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0940
- Référence CVE CAN-2004-1083 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1083
- Référence CVE CAN-2004-1084 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1084
- Référence CVE CAN-2004-0747 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0747
- Référence CVE CAN-2004-0786 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0786
- Référence CVE CAN-2004-0751 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0751
- Référence CVE CAN-2004-0748 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0748
- Référence CVE CAN-2004-1081 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1081
- Référence CVE CAN-2004-0803 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0803
- Référence CVE CAN-2004-0804 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0804
- Référence CVE CAN-2004-0886 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0886
- Référence CVE CAN-2004-1089 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1089
- Référence CVE CAN-2004-1085 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1085
- Référence CVE CAN-2004-0642 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0642
- Référence CVE CAN-2004-0643 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0643
- Référence CVE CAN-2004-0644 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0644
- Référence CVE CAN-2004-0772 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0772
- Référence CVE CAN-2004-1088 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1088
- Référence CVE CAN-2004-1086 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1086
- Référence CVE CAN-2004-1123 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1123

- Référence CVE CAN-2004-1121 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1121
- Référence CVE CAN-2004-1122 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1122
- Référence CVE CAN-2004-1087 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1087

Gestion détaillée du document

03 décembre 2004 version initiale.