Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 mai 2004
N° CERTA-2004-AVI-156

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Mac OS X

Conditions d'utilisation de ce document : http://www.certa.ssi.gouv.fr/certa/apropos.html
Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-156

Gestion du document

Référence	CERTA-2004-AVI-156
Titre	Multiples vulnérabilités dans Mac OS X
Date de la première version	06 mai 2004
Date de la dernière version	–
Source(s)	Avis de sécurité d'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

- Déni de service ;
- contournement de la politique de sécurité ;
- élévation de privilèges ;
- exécution de code arbitraire à distance ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

Mac OS X.

3 Résumé

De nombreuses vulnérabilités sont présentes dans certains composants de MAC OS X.

4 Description

Plusieurs vulnérabilités ont été découvertes dans Mac OS X :

- Apache 2 ne filtre pas les séquences d'échappement de terminaux dans ses journaux d'erreurs. Cette vulnérabilité peut être exploitée afin de modifier certains fichiers ou bien d'effectuer un déni de service ;
- deux vulnérabilités dans la mise en oeuvre d'IPSec permettent à un utilisateur mal intentionné de contourner la politique de sécurité ou d'effectuer un déni de service ;
- `AppleFileServer` fournit un système de partage de fichiers à partir du protocole AFP (Apple Filing Protocol). Une vulnérabilité dans la mise en oeuvre du système de pré-authentification permet à utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges `Root` ;
- `CoreFoundation` ne gére pas correctement les variables d'environnement.

5 Solution

Mettre à jour le système (cf. Documentation).

6 Documentation

- Avis de sécurité d'Apple :
  http://docs.info.apple.com/article.html?artnum=61798
- avis de sécurité atstake :
  http://www.atstake.com/research/advisories/2004/a050304-1.txt
- avis CERTA-2003-AVI-067 du CERTA "Vulnérabilité dans les émulateurs de terminaux" :
  http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-067/
- référence CVE CAN-2003-0020 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0020
- référence CVE CAN-2004-0113 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0113
- référence CVE CAN-2004-0155 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0155
- référence CVE CAN-2004-0174 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0174
- référence CVE CAN-2004-0403 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0403
- référence CVE CAN-2004-0428 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0428
- référence CVE CAN-2004-0429 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0429
- référence CVE CAN-2004-0430 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0430

Gestion détaillée du document

06 mai 2004 version initiale.