

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sous 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-2005-AVI-200>

Gestion du document

Référence	CERTA-2005-AVI-200
Titre	Multiples vulnérabilités sous Mac OS X
Date de la première version	09 juin 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité 2005-006 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

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

2 Systèmes affectés

- Apple Mac OS X 10.4.1 et versions antérieures.
- Apple Mac OS X 10.3.9 et versions antérieures (pour les vulnérabilités relatives à PHP et Bluetooth uniquement).

3 Description

Selon Apple, plusieurs composants du système d'exploitation Mac OS X présentent des vulnérabilités :

- Bluetooth : une vulnérabilité présente dans le service de transfert de fichiers (OBEX) permet d'accéder aux données du système situées hors du répertoire d'échange par défaut (CVE CAN-2005-1333) ;

- AFP : une faille de type débordement de mémoire est présente dans le service de fichiers AFP. Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code arbitraire à distance sur le serveur vulnérable (CVE CAN-2005-1721) ;
- CoreGraphics : une vulnérabilité est présente dans une routine gérant l'affichage des fichiers PDF. En incitant un utilisateur à visualiser un document habilement PDF constituée, il est possible de provoquer l'arrêt brutal de l'application utilisant la routine vulnérable (CVE CAN-2005-1722). De plus, une vulnérabilité permettant de réaliser une élévation de privilèges (CVE CAN-2005-1726) est également présente dans le serveur graphique ;
- des vulnérabilités liées à la mauvaise gestion des accès concurrents aux fichiers (CVE CAN-2005-1727, CVE CAN-2005-1725) peuvent être exploitées par un utilisateur local mal intentionné afin de réaliser une élévation de privilèges ;
- sous certaines conditions, la restriction d'accès aux volumes NFS exportés n'est pas cohérente avec celle spécifiée par l'utilisateur (CVE CAN-2005-1724) ;
- plusieurs vulnérabilités sont présentes dans le support PHP (CVE CAN-2005-0524, CVE CAN-2005-0525, CVE CAN-2005-1042, CVE CAN-2005-1043) ;
- une vulnérabilité de type débordement de mémoire présente dans l'exécutable `vpnd` peut être exploitée par un utilisateur local mal intentionné afin de réaliser une élévation de privilèges (CVE CAN-2005-1343).

4 Solution

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

5 Documentation

- Bulletin de sécurité Apple :
<http://docs.info.apple.com/article.html?artnum=301742>
- Référence CVE CAN-2005-0524 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0524>
- Référence CVE CAN-2005-0525 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0525>
- Référence CVE CAN-2005-1042 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1042>
- Référence CVE CAN-2005-1043 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1043>
- Référence CVE CAN-2005-1333 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1333>
- Référence CVE CAN-2005-1343 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1472>
- Référence CVE CAN-2005-1720 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1720>
- Référence CVE CAN-2005-1721 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1721>
- Référence CVE CAN-2005-1722 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1722>
- Référence CVE CAN-2005-1723 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1723>
- Référence CVE CAN-2005-1724 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1724>
- Référence CVE CAN-2005-1725 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1725>
- Référence CVE CAN-2005-1726 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1726>
- Référence CVE CAN-2005-1727 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1727>

- Référence CVE CAN-2005-1728 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1728>

Gestion détaillée du document

26 mai 2005 version initiale.