



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 mars 2007
N° CERTA-2007-AVI-124

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans MacOS 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-2007-AVI-124>

Gestion du document

Référence	CERTA-2007-AVI-124
Titre	Vulnérabilités dans MacOS X
Date de la première version	14 mars 2007
Date de la dernière version	–
Source(s)	Mise à jour de sécurité 2007-003 de MacOS X
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 ;
- exécution de code arbitraire ;
- déni de service à distance ;
- déni de service ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- MacOS X 10.3.9 et MacOS X Server 10.3.9 ;
- MacOS X 10.4 et MacOS X Server 10.4.

3 Résumé

Plusieurs vulnérabilités affectent MacOS X. Les plus graves permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Plusieurs composants de MacOS X sont sujets à des vulnérabilités, les plus graves permettant à un attaquant distant d'exécuter du code arbitraire.

Les composants impactés sont : ColorSync (CVE-2007-0719), CoreGraphics, Crash Reporter (CVE-2007-0467), CUPS (CVE-2007-0720), Disk Images (CVE-2007-0721, CVE-2007-0722, CVE-2006-6061, CVE-2006-6062, CVE-2006-5679, CVE-2007-0229, CVE-2007-0267, CVE-2007-0299), DS Plug-Ins (CVE-2007-0723), Flash Player (CVE-2006-5330), GNU Tar (CVE-2006-0300, CVE-2006-6097), HFS (CVE-2007-0318), HID Family (CVE-2007-0724), ImageIO (CVE-2007-1071, CVE-2007-0733), Kernel (CVE-2006-5836, CVE-2006-6129, CVE-2006-6173), MySQL Server (CVE-2006-1516, CVE-2006-1517, CVE-2006-2753, CVE-2006-3081, CVE-2006-4031, CVE-2006-4226, CVE-2006-3469), Networking (CVE-2006-6130, CVE-2007-0236), OpenSSH (CVE-2007-0726, CVE-2006-0225, CVE-2006-4924, CVE-2006-5051, CVE-2006-5052), Printing (CVE-2007-0728), QuickDraw Manager (CVE-2007-0588), servermgrd (CVE-2007-0730), SMB File Server (CVE-2007-0731), Software Update (CVE-2007-0463), sudo (CVE-2005-2959), WebLog (CVE-2006-4829).

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 12 mars 2007 :
<http://docs.info.apple.com/article.html?artnum=305214>
- Référence CVE CVE-2007-0719 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0719>
- Référence CVE CVE-2007-0467 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0467>
- Référence CVE CVE-2007-0720 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0720>
- Référence CVE CVE-2007-0721 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0721>
- Référence CVE CVE-2007-0722 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0722>
- Référence CVE CVE-2006-6061 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6061>
- Référence CVE CVE-2006-6062 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6062>
- Référence CVE CVE-2006-5679 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5679>
- Référence CVE CVE-2007-0229 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0229>
- Référence CVE CVE-2007-0267 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0267>
- Référence CVE CVE-2007-0299 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0299>
- Référence CVE CVE-2007-0723 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0723>
- Référence CVE CVE-2006-5330 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5330>
- Référence CVE CVE-2006-0300 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0300>

- Référence CVE CVE-2006-6097 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6097>
- Référence CVE CVE-2007-0318 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0318>
- Référence CVE CVE-2007-0724 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0724>
- Référence CVE CVE-2007-1071 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1071>
- Référence CVE CVE-2007-0733 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0733>
- Référence CVE CVE-2006-5836 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5836>
- Référence CVE CVE-2006-6129 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6129>
- Référence CVE CVE-2006-6173 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6173>
- Référence CVE CVE-2006-1516 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1516>
- Référence CVE CVE-2006-1517 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1517>
- Référence CVE CVE-2006-2753 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2753>
- Référence CVE CVE-2006-3081 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3081>
- Référence CVE CVE-2006-4031 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4031>
- Référence CVE CVE-2006-4226 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4226>
- Référence CVE CVE-2006-3469 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3469>
- Référence CVE CVE-2006-6130 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6130>
- Référence CVE CVE-2007-0236 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0236>
- Référence CVE CVE-2007-0726 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0726>
- Référence CVE CVE-2006-0225 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0225>
- Référence CVE CVE-2006-4924 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4924>
- Référence CVE CVE-2006-5051 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5051>
- Référence CVE CVE-2006-5052 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5052>
- Référence CVE CVE-2007-0728 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0728>
- Référence CVE CVE-2007-0588 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0588>
- Référence CVE CVE-2007-0730 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0730>
- Référence CVE CVE-2007-0731 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0731>

- Référence CVE CVE-2007-0463 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0463>
- Référence CVE CVE-2005-2959 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2959>
- Référence CVE CVE-2006-4829 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4829>

Gestion détaillée du document

14 mars 2007 version initiale.