



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 août 2007
N° CERTA-2007-AVI-340

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Apple 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-2007-AVI-340>

Gestion du document

Référence	CERTA-2007-AVI-340
Titre	Multiples vulnérabilités dans Apple Mac OS X
Date de la première version	01 août 2007
Date de la dernière version	–
Source(s)	Avis de sécurité Apple 2007-007 306172 du 30 juillet 2007
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Apple Mac OS X v10.3.9 ;
- Apple Mac OS X Server v10.3.9 ;
- Apple Mac OS X v10.4.10 ;
- Apple Mac OS X Server v10.4.10.

3 Résumé

Plusieurs vulnérabilités ont été identifiées : elles concernent le système d'exploitation Mac OS X. L'exploitation de ces dernières peut avoir des conséquences variées, comme l'exécution de code arbitraire, ou un dysfonctionnement du système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le système d'exploitation Mac OS X. Parmi celles-ci :

- `bzip2` : un nom d'archive malicieusement formé permet l'exécution de code arbitraire à distance ;
- `CFNetwork` : un clic sur une adresse malicieusement formée permet l'exécution de commandes FTP arbitraires à distance ;
- `CoreAudio` : une page Web malicieusement créée permet à l'aide d'une applet Java d'exécuter du code arbitraire à distance ;
- `cscope` : des vulnérabilités concernant un dépassement de mémoire et la création de fichiers temporaires dangereux ont été corrigées ;
- `gnuzip` : un nom d'archive malicieusement formé permet l'exécution de code arbitraire à distance ;
- `iChat` : un dépassement de mémoire permet de provoquer un déni de service à distance ou l'exécution de code arbitraire à distance au sein d'un même sous réseau ;
- `Kerberos` : des vulnérabilités pouvant provoquer un déni de service ou l'exécution de code arbitraire à distance ont été corrigées ;
- `mDNSResponder` : un dépassement de mémoire permet de provoquer un déni de service à distance ou l'exécution de code arbitraire à distance au sein d'un même sous réseau ;
- `PDFKit` : l'ouverture d'un document malicieusement créé permet un déni de service de l'application ou l'exécution de code arbitraire ;
- `PHP` : plusieurs vulnérabilités touchant PHP 4.4.4 ont été corrigées ;
- `Quartz Composer` : l'ouverture d'un fichier Quartz malicieusement créé permet un déni de service de l'application ou l'exécution de code arbitraire ;
- `Samba` : lorsque le partage de fichiers Windows est activé, un utilisateur non authentifié peut, à distance, provoquer un déni de service, exécuter du code ou des commandes arbitraires et contourner la politique de sécurité ;
- `SquirrelMail` : plusieurs vulnérabilités dont au moins une permettant une attaque de type *cross-site scripting* ont été corrigées ;
- `Tomcat` : plusieurs vulnérabilités dont certaines permettant des attaques de type *cross-site scripting* et l'atteinte à la confidentialité des données ont été corrigées ;
- `WebCore` : des vulnérabilités permettant l'exécution d'applets Java alors que celui-ci est désactivé et permettant la réalisation d'attaques de type *cross-site scripting* ont été corrigées ;
- `WebKit` : l'ouverture d'une page Web malicieusement créée permet l'exécution de code arbitraire à distance.

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 2007-007 306172 du 30 juillet 2007 :
<http://docs.info.apple.com/article.html?artnum=306172>
- Référence CVE CVE-2004-0996 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0996>
- Référence CVE CVE-2004-2541 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2541>
- Référence CVE CVE-2005-0758 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0758>
- Référence CVE CVE-2005-0758 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0758>
- Référence CVE CVE-2005-2090 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2090>

- Référence CVE CVE-2005-3128 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3128>
- Référence CVE CVE-2006-2842 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2842>
- Référence CVE CVE-2006-3174 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3174>
- Référence CVE CVE-2006-4019 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4019>
- Référence CVE CVE-2006-6142 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6142>
- Référence CVE CVE-2007-0450 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0450>
- Référence CVE CVE-2007-0478 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0478>
- Référence CVE CVE-2007-1001 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1001>
- Référence CVE CVE-2007-1262 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1262>
- Référence CVE CVE-2007-1287 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1287>
- Référence CVE CVE-2007-1358 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1358>
- Référence CVE CVE-2007-1460 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1460>
- Référence CVE CVE-2007-1461 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1461>
- Référence CVE CVE-2007-1484 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1484>
- Référence CVE CVE-2007-1521 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1521>
- Référence CVE CVE-2007-1583 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1583>
- Référence CVE CVE-2007-1711 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1711>
- Référence CVE CVE-2007-1717 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1717>
- Référence CVE CVE-2007-1860 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1860>
- Référence CVE CVE-2007-2403 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2403>
- Référence CVE CVE-2007-2404 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2404>
- Référence CVE CVE-2007-2405 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2405>
- Référence CVE CVE-2007-2406 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2406>
- Référence CVE CVE-2007-2407 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2407>
- Référence CVE CVE-2007-2408 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2408>
- Référence CVE CVE-2007-2409 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2409>

- Référence CVE CVE-2007-2410 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2410>
- Référence CVE CVE-2007-2442 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2442>
- Référence CVE CVE-2007-2443 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2443>
- Référence CVE CVE-2007-2446 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2446>
- Référence CVE CVE-2007-2447 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2447>
- Référence CVE CVE-2007-2589 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2589>
- Référence CVE CVE-2007-2798 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2798>
- Référence CVE CVE-2007-3742 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3742>
- Référence CVE CVE-2007-3744 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3744>
- Référence CVE CVE-2007-3745 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3745>
- Référence CVE CVE-2007-3745 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3745>
- Référence CVE CVE-2007-3746 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3746>
- Référence CVE CVE-2007-3747 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3747>
- Référence CVE CVE-2007-3748 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3748>
- Référence CVE CVE-2007-3944 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3944>

Gestion détaillée du document

01 août 2007 version initiale.