



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 2008
N° CERTA-2008-AVI-388

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-2008-AVI-388>

Gestion du document

Référence	CERTA-2008-AVI-388
Titre	Multiples vulnérabilités dans Mac OS X
Date de la première version	01 août 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT2647 du 1 août 2008
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

- Mac OS X Server 10.4 ;
- Mac OS X 10.4.11 ;
- Mac OS X Server 10.5 ;
- Mac OS X 10.5.4.

3 Résumé

Plusieurs vulnérabilités permettant entre autres l'exécution de code arbitraire à distance, et concernant le système d'exploitation Mac OS X, ont été corrigées.

4 Description

Plusieurs vulnérabilités concernant Mac OS X ont été corrigées :

- Open Scripting Architecture : une mauvaise gestion des droits des *plugins* permet à un utilisateur malveillant local d'élever ses privilèges.
- BIND : une mauvaise gestion de l'aléa et un vulnérabilité protocolaire permettent de corrompre le cache du DNS.
- CarbonCore : une vulnérabilité dans les gestion des noms longs de fichier permet l'exécution de code arbitraire.
- CoreGraphics : une corruption de mémoire permet l'exécution de code arbitraire, par exemple à l'aide d'un site Web spécifiquement réalisé.
- CoreGraphics : un dépassement d'entier lors de la gestion de fichiers au format PDF permet l'exécution de code arbitraire.
- Data Detectors Engine : la visualisation d'un message spécifiquement créé permet de provoquer un déni de service de l'application.
- Disk Utility : après l'utilisation de l'outil *Repair Permissions* il est possible d'exécuter des commandes avec les droits système à l'aide d'*emacs*.
- OpenLDAP : un message spécifiquement réalisé permet de provoquer un déni de service de l'application.
- OpenSSL : une vulnérabilité dans la fonction *SSL_get_shared_ciphers()* permet de provoquer un déni de service de l'application.
- PHP : plusieurs vulnérabilités, dont certaines permettant l'exécution de code arbitraire, ont été corrigées.
- QuickLook : un document au format Microsoft Office spécifiquement réalisé permet l'exécution de code arbitraire.
- rsync : l'utilisation de liens symboliques permet de modifier des fichiers hors du module.

5 Solution

Se référer au bulletin de sécurité d'Apple HT2647 du 1 août 2008 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple HT2647 du 01 août 2008 :
<http://support.apple.com/kb/HT2647>
- Référence CVE CVE-2007-4850 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4850>
- Référence CVE CVE-2007-5135 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5135>
- Référence CVE CVE-2007-6199 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6199>
- Référence CVE CVE-2007-6200 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6200>
- Référence CVE CVE-2008-0599 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0599>
- Référence CVE CVE-2008-0674 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0674>
- Référence CVE CVE-2008-1447 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447>
- Référence CVE CVE-2008-2050 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2050>
- Référence CVE CVE-2008-2051 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2051>
- Référence CVE CVE-2008-2320 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2320>

- Référence CVE CVE-2008-2321 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2321>
- Référence CVE CVE-2008-2322 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2322>
- Référence CVE CVE-2008-2323 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2323>
- Référence CVE CVE-2008-2324 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2324>
- Référence CVE CVE-2008-2325 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2325>
- Référence CVE CVE-2008-2952 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2952>

Gestion détaillée du document

01 août 2008 version initiale.