Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 juillet 2008
N° CERTA-2008-AVI-343

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-2008-AVI-343

Gestion du document

Référence	CERTA-2008-AVI-343
Titre	Multiples vulnérabilités dans Apple Mac OS X
Date de la première version	02 juillet 2008
Date de la dernière version	–
Source(s)	Mise à jour de sécurité Apple 2008-004 du 30 juin 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 ;
- élévation de privilèges.

2 Systèmes affectés

Apple Mac OS X versions v10.5.3 et antérieures.

3 Résumé

Plusieurs vulnérablités concernant le système d'exploitation Apple Mac OS X ont été corrigées.

4 Description

Plusieurs vulnérablités ont été corrigées :

– `Alias Manager` : un alias spécifiquement créé permet l'exécution de code arbitraire ;

- `CoresTypes` : des contenus incertains peuvent être ouverts automatiquement ;
- `c++filt` : une chaine de caratères spécifiquement créée permet l'exécution de code arbitraire ;
- `Dock` : une personne ayant physiquement accès à la machine peut contourner l'écran de verrouillage ;
- `Launch Services` : du code malveillant peut être exécuté via un site Web malveillant ;
- `Net-SNMP` : il est possible de contrefaire un paquet *SNMPv3* ;
- `Ruby` : une chaine de caractères ou un tableau spécifiquement créé permet l'exécution de code arbitraire ;
- `SMB File Server` : une trame *SMB* spécialement réalisée permet l'exécution de code arbitraire ;
- `System Configuration` : un utilisateur local peut exécuter du code arbitraire avec les droits de nouveaux utilisateurs ;
- `Tomcat` : plusieurs vulnérabilités affectent le logiciel dont une permettant des attaques de type *Cross Site Scripting* ;
- `VPN` : un attaquant peut réaliser un déni de service à distance à l'aide de paquets *UDP* spécifiquement créés ;
- `Webkit` : du code malveillant peut être exécuté via un site Web malveillant.

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 2008-004 du 30 juin 2008 :
  http://support.apple.com/kb/HT2163
- Référence CVE CVE-2005-3164 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3164
- Référence CVE CVE-2007-1355 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1355
- Référence CVE CVE-2007-2449 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2449
- Référence CVE CVE-2007-2450 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2450
- Référence CVE CVE-2007-3382 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3382
- Référence CVE CVE-2007-3383 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3383
- Référence CVE CVE-2007-3385 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3385
- Référence CVE CVE-2007-5333 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5333
- Référence CVE CVE-2007-5461 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5461
- Référence CVE CVE-2007-6276 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6276
- Référence CVE CVE-2008-0960 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0960
- Référence CVE CVE-2008-1105 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1105
- Référence CVE CVE-2008-1145 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1145
- Référence CVE CVE-2008-2307 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2307
- Référence CVE CVE-2008-2308 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2308

- Référence CVE CVE-2008-2309 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2309
- Référence CVE CVE-2008-2310 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2310
- Référence CVE CVE-2008-2311 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2311
- Référence CVE CVE-2008-2313 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2313
- Référence CVE CVE-2008-2314 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2314
- Référence CVE CVE-2008-2662 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2662
- Référence CVE CVE-2008-2663 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2663
- Référence CVE CVE-2008-2664 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2664
- Référence CVE CVE-2008-2725 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2725
- Référence CVE CVE-2008-2726 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2726

Gestion détaillée du document

02 juillet 2008 version initiale.