Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2005
N° CERTA-2005-AVI-258

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-2005-AVI-258

Gestion du document

Référence	CERTA-2005-AVI-258
Titre	Multiples vulnérabilités dans Mac OS X
Date de la première version	13 juillet 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple #301948 du 11 juillet 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

- Mac OS X v10.4 ;
- Mac OS X Server v10.4.

3 Résumé

Deux vulnérabilités découvertes dans Mac OS X permettent à un utilisateur mal intentionné de réaliser à distance un déni de service ou de porter atteinte à l'intégrité des données.

4 Description

Deux vulnérabilités ont été découvertes dans le système d'exploitation Mac OS X d'Apple :

- la première vulnérabilité est dûe à une erreur de gestion des paquets TCP/IP. Une personne malveillante peut exploiter cette vulnérabilité au moyen de paquets TCP/IP malicieusement construits afin de figer le système et de forcer l'utilisateur à le redémarrer (CAN-2005-2194) ;
- la seconde vulnérabilité présente dans l'application `Dashboard` permet à un utilisateur mal intentionné de contourner la politique de sécurité et de porter atteinte à l'intégrité des données, en écrasant des `widget` pré-installés. Cette vulnérabilité peut être exploitée au moyen d'un `widget` dont l'identifiant interne est malicieusement constitué (CAN-2005-1333).

5 Solution

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

6 Documentation

- Site internet d'apple :
  http://www.apple.com
- Bulletin de sécurité Apple #301948 du 11 juillet 2005 :
  http://docs.info.apple.com/article.html?artnum=301948
- Référence CVE CAN-2005-2194 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2194
- Référence CVE CAN-2005-1333 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1333

Gestion détaillée du document

13 juillet 2005 version initiale.