



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 16 février 2007  
N° CERTA-2006-ALE-013-002

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

**Objet : Vulnérabilités de 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-2006-ALE-013>

---

### Gestion du document

Référence	CERTA-2006-ALE-013-002
Titre	Vulnérabilité de MacOS X
Date de la première version	23 novembre 2006
Date de la dernière version	14 février 2007
Source(s)	Avis Secunia SA23012
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

- Déni de service à distance ;
- élévation de privilèges.

### 2 Systèmes affectés

- Apple Macintosh OS X

### 3 Résumé

Une mauvaise gestion des fichiers d'image disque (format DMG) permet à un utilisateur d'obtenir des privilèges élevés et de compromettre l'ordinateur à l'aide d'un fichier corrompu.

### 4 Description

Plusieurs vulnérabilités ont été identifiées, en relation avec le format DMG sous Apple MacOS X. Parmi celles-ci :

- le mauvais traitement des fichiers corrompus d'image disque (format DMG) par la fonction `com.apple.`

- AppleDiskImageController peut provoquer un déni de service ;
- Apple Finder ne manipulerait pas correctement des fichiers d'image dont le nom de volume dépasse 255 octets ;
  - le système de fichiers UFS aurait plusieurs fonctions vulnérables à des attaques de type débordement d'entiers (ou *integer overflow*) : `ffs_mountfs()` et `byte_swap_sbin()` ;
  - l'appel à la fonction `ufs_dirbad()` par `ufs_lookup()` pourrait provoquer, sous certaines conditions, un déni de service du système vulnérable ;
  - une image DMG contenant un système de fichiers UFS+ et construite de manière particulière pourrait provoquer un dysfonctionnement du système vulnérable, suite à l'appel à la fonction `do_hfs_truncate()`.

Des codes exploitant ces vulnérabilités circulent sur Internet.

## 5 Contournement provisoire

- N'autoriser l'accès au système vulnérable qu'aux personnes de confiance ;
- limiter le téléchargement de fichiers DMG et en vérifier l'intégrité avant installation ;
- désactiver l'option de Safari : Ouvrir automatiquement les fichiers « fiables » et les options équivalentes des autres navigateurs.

## 6 Solution

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

## 7 Documentation

- Mise à jour de sécurité Apple 2007-002 du 15 février 2007 :  
<http://docs.info.apple.com/article.html?artnum=305102>
- Bulletin de sécurité Secunia du 21 novembre 2006 :  
<http://secunia.com/advisories/23012>
- Référence CVE CVE-2007-0299 :  
<http://www.cve-mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0299>
- Référence CVE CVE-2007-0267 :  
<http://www.cve-mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0267>
- Référence CVE CVE-2007-0197 :  
<http://www.cve-mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0197>
- Référence CVE CVE-2006-5679 :  
<http://www.cve-mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5679>
- Référence CVE CVE-2006-5482 :  
<http://www.cve-mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5482>

## Gestion détaillée du document

**23 novembre 2006** version initiale.

**22 janvier 2007** ajout de nouvelles vulnérabilités et références.

**16 février 2007** ajout de la mise à jour Apple.