



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 06 août 2009  
N° CERTA-2009-AVI-309

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités du système d'exploitation Apple 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-2009-AVI-309>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2009-AVI-309   |
| Titre                       | Multiples vulnérabilités du système d'exploitation Apple MacOS X |
| Date de la première version | 06 août 2009   |
| Date de la dernière version | –  |
| Source(s)                   | Bulletin de sécurité Apple numéro HT3757 du 05 août 2009         |
| 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.

## 2 Systèmes affectés

- MacOS X version 10.4.11 et versions antérieures ;
- MacOS X version 10.5.7 et versions antérieures ;
- MacOS X Server version 10.4.11 et versions antérieures ;
- MacOS X Server version 10.5.7 et versions antérieures.

## 3 Résumé

De multiples vulnérabilités permettant, entre autres, l'exécution de code arbitraire à distance ont été découvertes dans le système d'exploitation MacOS X d'Apple.

## 4 Description

De multiples vulnérabilités ont été découvertes dans le système d'exploitation macOS X d'Apple. L'exploitation de ces vulnérabilités permet à un utilisateur mal intentionné de contourner la politique de sécurité, de réaliser un déni de service à distance ou encore de prendre le contrôle à distance d'une machine vulnérable.

## 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 numéro HT3757 du 05 août 2009 :  
<http://support.apple.com/kb/HT3757>
- Référence CVE CVE-2008-0674 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0674>
- Référence CVE CVE-2008-1372 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1372>
- Référence CVE CVE-2009-0040 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0040>
- Référence CVE CVE-2009-0151 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0151>
- Référence CVE CVE-2009-1235 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1235>
- Référence CVE CVE-2009-1720 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1720>
- Référence CVE CVE-2009-1721 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1721>
- Référence CVE CVE-2009-1722 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1722>
- Référence CVE CVE-2009-1723 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1723>
- Référence CVE CVE-2009-1726 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1726>
- Référence CVE CVE-2009-1727 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1727>
- Référence CVE CVE-2009-1728 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1728>
- Référence CVE CVE-2009-2188 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2188>
- Référence CVE CVE-2009-2190 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2190>
- Référence CVE CVE-2009-2191 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2191>
- Référence CVE CVE-2009-2192 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2192>
- Référence CVE CVE-2009-2193 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2193>
- Référence CVE CVE-2009-2194 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2194>

## Gestion détaillée du document

06 août 2009 version initiale.