

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Apple iChat

---

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-2007-AVI-091>

---

### Gestion du document

Référence	CERTA-2007-AVI-091
Titre	Multiples vulnérabilités dans Apple iChat
Date de la première version	16 février 2007
Date de la dernière version	–
Source(s)	Mise à jour de sécurité Apple 2007-002 du 15 février 2007
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.

## 2 Systèmes affectés

- Mac OS X et Mac OS X Server version 10.3.9 ;
- Mac OS X et Mac OS X Server version 10.4.8.

## 3 Résumé

Plusieurs vulnérabilités présentes dans iChat peuvent permettre de réaliser un déni de service ou l'exécution de code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités ont été identifiées dans iChat :

- un problème de validation lors de l'échange du message Bonjour (CVE-2007-0614 et CVE-2007-0710)

permet à un utilisateur malintentionné du réseau local de réaliser un déni de service de l'application iChat par le biais d'un message Bonjour spécialement conçu ;

- un manque de validation des adresses réticulaires AIM d'iChat (CVE-2007-0021) peut permettre à un utilisateur distant malintentionné de réaliser un déni de service de l'application iChat ou d'exécuter du code arbitraire par le biais d'une adresse réticulaire AIM spécialement conçue.

## 5 Solution

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

## 6 Documentation

- Mise à jour de sécurité Apple 2007-002 du 15 février 2007 :  
<http://docs.info.apple.com/article.html?artnum=305102>
- Référence CVE CVE-2007-0614 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0614>
- Référence CVE CVE-2007-0710 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0710>
- Référence CVE CVE-2007-0021 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0021>

## Gestion détaillée du document

16 février 2007 version initiale.