

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Apple QuickTime et iPhoto

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-059>

Gestion du document

Référence	CERTA-2008-AVI-059
Titre	Vulnérabilités dans Apple QuickTime et iPhoto
Date de la première version	07 février 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité Apple 307407 et 307398 du 04 février 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.

2 Systèmes affectés

- Les versions d'Apple QuickTime antérieures à 7.4.1 ;
- les versions d'Apple iPhoto antérieures à 7.1.2.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les applications Apple QuickTime et iPhoto. L'une d'elles a d'ailleurs fait l'objet de l'alerte CERTA-2008-ALE-001 publiée le 11 janvier 2008.

Les conséquences de l'exploitation de ces vulnérabilités sont variées, permettant pour certaines d'exécuter du code arbitraire à distance sur un système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans les applications Apple QuickTime et iPhoto.

L'une d'elles, sur QuickTime, a d'ailleurs fait l'objet de l'alerte CERTA-2008-ALE-001 publiée le 11 janvier 2008. Elle concerne un dépassement de mémoire tampon lors d'une tentative infructueuse de lecture de lecture d'un fichier via le protocole *Real Time Streaming Protocol* (RTSP).

iPhoto, quant à lui, ne manipulerait pas correctement certaines diffusions de photos (*photocast*) spécialement construites.

5 Solution

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

6 Documentation

- Document du CERTA CERTA-2008-ALE-001 du 14 janvier 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-001/index.html>
- Bulletin de sécurité Apple 307407 du 04 février 2008 :
<http://docs.info.apple.com/article.html?artnum=307407>
- Bulletin de sécurité Apple 307398 du 04 février 2008 :
<http://docs.info.apple.com/article.html?artnum=307398>
- Référence CVE CVE-2008-0234 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0234>
- Référence CVE CVE-2008-0043 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0043>

Gestion détaillée du document

07 février 2008 version initiale.