



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 janvier 2006
N° CERTA-2006-AVI-019

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans QuickTime

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-AVI-019>

Gestion du document

Référence	CERTA-2006-AVI-019
Titre	Vulnérabilités dans QuickTime
Date de la première version	11 janvier 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple du 10 janvier 2006
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.

2 Systèmes affectés

QuickTime versions 7.0.3 et antérieures.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans QuickTime permettant l'exécution de code arbitraire à distance ou la réalisation d'un déni de service.

4 Description

- Une vulnérabilité a été découverte dans le traitement des images au format QTIF (QuickTime Image). Un utilisateur mal intentionné peut, par le biais d'une image au format QTIF malicieusement constituée, exécuter du code arbitraire à distance (CVE-2005-2340) ;

- une vulnérabilité a été découverte dans le traitement des images au format TGA (Truevision Targa Graphic). Un utilisateur mal intentionné peut, par le biais d'une image au format TGA malicieusement constituée, exécuter du code arbitraire à distance ou réaliser un déni de service (CVE-2005-3707, CVE-2005-3708, CVE-2005-3709);
- une vulnérabilité a été découverte dans le traitement des images au format TIFF (Tagged Image File Format). Un utilisateur mal intentionné peut, par le biais d'une image au format TIFF malicieusement constituée, exécuter du code arbitraire à distance ou réaliser un déni de service (CVE-2005-3710, CVE-2005-3711);
- une vulnérabilité a été découverte dans le traitement des images au format GIF (Graphic Interchange Format). Un utilisateur mal intentionné peut, par le biais d'une image au format GIF malicieusement constituée, exécuter du code arbitraire à distance (CVE-2005-3713);
- une vulnérabilité a été découverte dans le traitement des fichiers media. Un utilisateur mal intentionné peut, par le biais d'un fichier media malicieusement constitué, exécuter du code arbitraire à distance (CVE-2005-4092).

5 Solution

Mettre à jour QuickTime en version 7.0.4 (voir Documentation).

6 Documentation

- Téléchargement de la version 7.0.4 de QuickTime :
<http://www.apple.com/quicktime>
- Bulletin de sécurité Apple du 10 janvier 2006 :
<http://docs.info.apple.com/article.html?artnum=61798>
- Référence CVE CVE-2005-2340 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2340>
- Référence CVE CVE-2005-3707 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3707>
- Référence CVE CVE-2005-3708 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3708>
- Référence CVE CVE-2005-3709 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3709>
- Référence CVE CVE-2005-3710 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3710>
- Référence CVE CVE-2005-3711 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3711>
- Référence CVE CVE-2005-3713 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3713>
- Référence CVE CVE-2005-4092 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4092>

Gestion détaillée du document

11 janvier 2006 version initiale.