

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Apple 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-2011-AVI-597>

Gestion du document

Référence	CERTA-2011-AVI-597
Titre	Vulnérabilités dans Apple QuickTime
Date de la première version	28 octobre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT5016 du 26 octobre 2011
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 ;
- contournement de la politique de sécurité ;
- injection de code indirecte à distance.

2 Systèmes affectés

QuickTime versions inférieures à la version 7.7.1 pour Windows.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans Apple QuickTime pour Windows. Elles permettaient à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été corrigées dans Apple QuickTime pour Windows. Les plus critiques permettaient à une personne malintentionnée d'exécuter du code arbitraire à distance au moyen d'une vidéo spécialement conçue.

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 HT5016 du 26 octobre 2011 :
<http://support.apple.com/kb/HT5016>
- Référence CVE CVE-2011-3218 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3218>
- Référence CVE CVE-2011-3219 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3219>
- Référence CVE CVE-2011-3220 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3220>
- Référence CVE CVE-2011-3221 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3221>
- Référence CVE CVE-2011-3222 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3222>
- Référence CVE CVE-2011-3223 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3223>
- Référence CVE CVE-2011-3228 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3228>
- Référence CVE CVE-2011-3247 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3247>
- Référence CVE CVE-2011-3248 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3248>
- Référence CVE CVE-2011-3249 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3249>
- Référence CVE CVE-2011-3250 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3250>
- Référence CVE CVE-2011-3251 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3251>

Gestion détaillée du document

28 octobre 2011 version initiale.