

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Apple iTunes

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-2010-AVI-270>

Gestion du document

Référence	CERTA-2010-AVI-270
Titre	Multiples vulnérabilités dans Apple iTunes
Date de la première version	17 juin 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT4220 du 16 juin 2010
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.

2 Systèmes affectés

Apple iTunes versions antérieures à 9.2.

3 Résumé

Plusieurs vulnérabilités découvertes dans iTunes peuvent être exploitées par un utilisateur malintentionné afin de compromettre le système.

4 Description

De multiples vulnérabilités ont été découvertes dans iTunes :

- une erreur dans le module `colorsync` peut conduire à une exécution de code arbitraire lors de l'ouverture d'une image spécialement conçue ;

- l'ouverture d'image au format `tiff` malveillante peut aussi entrainer une execution de code arbitraire ;
- la version de `webkit` embarquée dans `iTunes` est vulnérable à des attaques connues.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). La version 9.2 du logiciel corrige ces problèmes.

6 Documentation

- Bulletin de sécurité Apple HT4220 du 16 juin 2010 :
<http://support.apple.com/kb/HT4220>
- Référence CVE CVE-2009-1726 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1726>
- Référence CVE CVE-2010-0544 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0544>
- Référence CVE CVE-2010-1119 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1119>
- Référence CVE CVE-2010-1387 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1387>
- Référence CVE CVE-2010-1390 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1390>
- Référence CVE CVE-2010-1392 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1392>
- Référence CVE CVE-2010-1393 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1393>
- Référence CVE CVE-2010-1395 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1395>
- Référence CVE CVE-2010-1396 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1396>
- Référence CVE CVE-2010-1397 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1397>
- Référence CVE CVE-2010-1398 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1398>
- Référence CVE CVE-2010-1399 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1399>
- Référence CVE CVE-2010-1400 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1400>
- Référence CVE CVE-2010-1401 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1401>
- Référence CVE CVE-2010-1402 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1402>
- Référence CVE CVE-2010-1403 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1403>
- Référence CVE CVE-2010-1404 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1404>
- Référence CVE CVE-2010-1405 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1405>
- Référence CVE CVE-2010-1408 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1408>
- Référence CVE CVE-2010-1409 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1409>

- Référence CVE CVE-2010-1410 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1410>
- Référence CVE CVE-2010-1411 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1411>
- Référence CVE CVE-2010-1412 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1412>
- Référence CVE CVE-2010-1414 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1414>
- Référence CVE CVE-2010-1415 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1415>
- Référence CVE CVE-2010-1416 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1416>
- Référence CVE CVE-2010-1417 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1417>
- Référence CVE CVE-2010-1418 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1418>
- Référence CVE CVE-2010-1419 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1419>
- Référence CVE CVE-2010-1421 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1421>
- Référence CVE CVE-2010-1422 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1422>
- Référence CVE CVE-2010-1749 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1749>
- Référence CVE CVE-2010-1758 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1758>
- Référence CVE CVE-2010-1759 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1759>
- Référence CVE CVE-2010-1761 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1761>
- Référence CVE CVE-2010-1763 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1763>
- Référence CVE CVE-2010-1769 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1769>
- Référence CVE CVE-2010-1770 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1770>
- Référence CVE CVE-2010-1771 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1771>
- Référence CVE CVE-2010-1774 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1774>

Gestion détaillée du document

17 juin 2010 version initiale.