Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 août 2010
N° CERTA-2010-AVI-380

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Apple iOS

Gestion du document

Référence	CERTA-2010-AVI-380
Titre	Multiples vulnérabilités dans Apple iOS
Date de la première version	12 août 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT4291 du 11 août 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 ;
- déni de service à distance ;
- élévation de privilèges.

2 Systèmes affectés

- iPhone avec iOS 3.1.2 à 4.0.1 ;
- iPad avec iOS 3.2 à 3.2.1 ;
- iPod Touch avec iOS 3.1.2 à 4.0.

3 Résumé

Deux vulnérabilités présentes dans `Apple iOS` permettent à un utilisateur distant malintentionné de provoquer un déni de service, d'exécuter du code arbitraire et d'élever ses privilèges.

4 Description

Deux vulnérabilités sont présentes dans le système embarqué `iOS` de `Apple` :

- la première (CVE-2010-1797) est relative à la mise en œuvre du support des fichiers au format `PDF`. Elle permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire au moyen d'un fichier `PDF` contenant une police de type `FreeType` construite de façon particulière ;
- la seconde (CVE-2010-2973) concerne le composant *IOSurface* du système et permet à un utilisateur standard d'élever ses privilèges jusqu'au niveau système.

Ces deux vulnérabilités ont fait l'objet de l'alerte CERTA-2010-ALE-011 et sont, à la date de cette publication, activement exploitées de façon combinées sur l'Internet afin de compromettre des équipements vulnérables.

5 Solution

La version 4.0.2 de l'iOS corrige le problème.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple HT4291 du 11 août 2010 :
  http://support.apple.com/kb/HT4291
- Document du CERTA CERTA-2010-ALE-011 du 04 août 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-011/index.html
- Référence CVE CVE-2010-1797 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1797
- Référence CVE CVE-2010-2973 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2973

Gestion détaillée du document

12 août 2010 version initiale.