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-ALE-011-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilités dans Apple iOS

Gestion du document

Référence	CERTA-2010-ALE-011-001
Titre	Vulnérabilités dans Apple iOS
Date de la première version	04 août 2010
Date de la dernière version	12 août 2010
Source(s)	–
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.
- 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 non corrigées ont été découvertes dans l'Apple iOS.
Un correctif a été publié le 11 août 2010.

4 Description

Deux vulnérabilités ont été découvertes dans l'Apple iOS. La première concerne le traitement des fichiers au format PDF et permet l'exécution de code arbitraire à distance. La seconde est une vulnérabilité du noyau utilisable pour effectuer une élévation de privilèges. La combinaison des deux permet à une personne malintentionnée d'exécuter du code arbitraire à distance avec les droits administrateur et d'accéder ainsi à l'ensemble des informations (*contacts, mails, documents ...*) et ressources (*caméra, micro, GPS...*) de l'appareil. Cette vulnérabilité est entre autre utilisée pour effectuer le *Jailbreak*.

5 Contournement provisoire

En attendant le correctif d'Apple, il est recommandé la plus grande prudence lors de l'ouverture de fichiers au format PDF, par exemple en n'ouvrant que des fichiers attendus ou en validant la légitimité du message auprès de l'envoyeur.

6 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).

7 Documentation

- Bulletin de sécurité Apple HT4291 du 11 août 2010 :
  http://support.apple.com/kb/HT4291
- Document du CERTA CERTA-2010-AVI-011 du 04 août 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-380/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

04 août 2010 version initiale ;
12 août 2010 ajout de la solution et de la section documentation.