

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilités dans Apple iOS

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-ALE-004>

Gestion du document

Référence	CERTA-2011-ALE-004-001
Titre	Vulnérabilités dans Apple iOS
Date de la première version	05 juillet 2011
Date de la dernière version	18 juillet 2011
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 4, 3GS et 3G avec iOS versions 4.3.3 et antérieures ;
- iPad 1G et 2 avec iOS versions 4.3.3 et antérieures ;
- iPod Touch 2G, 3G et 4G avec iOS versions 4.3.3 et antérieures.

3 Résumé

Deux vulnérabilités non corrigées ont été découvertes dans l'Apple iOS.

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. Des preuves de faisabilité circulent déjà sur l'Internet. Ces vulnérabilités sont, entre autre, utilisées 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'expéditeur.

6 Solution

Se référer au bulletin de sécurité Apple HT4802 et HT4803 pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Apple HT4802 du 15 juillet 2011 :
<http://support.apple.com/kb/HT4802>
- Bulletin de sécurité Apple HT4803 du 15 juillet 2011 :
<http://support.apple.com/kb/HT4803>
- Référence CVE CVE-2010-3855 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3855>
- Référence CVE CVE-2011-0226 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0226>
- Référence CVE CVE-2011-0227 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0227>

Gestion détaillée du document

05 juillet 2011 version initiale.

18 juillet 2011 ajout des références aux bulletins Apple et aux CVE.