

Affaire suivie par :  
CERTA

## AVIS 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-AVI-395>

---

### Gestion du document

Référence	CERTA-2011-AVI-395
Titre	Vulnérabilités dans Apple iOS
Date de la première version	18 juillet 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité Apple HT4802 et HT4803 du 15 juillet 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 ;
- élévation de privilèges.

## 2 Systèmes affectés

- Apple iOS versions 4.2.5 à 4.2.8 pour iPhone 4 modèle CDMA ;
- Apple iOS versions 3.0 à 4.3.3 pour iPhone 3GS et iPhone 4 modèle GSM ;
- Apple iOS versions 3.1 à 4.3.3 pour iPod touch de 3ème génération et postérieures ;
- Apple iOS versions 3.2 à 4.3.3 pour iPad.

## 3 Résumé

Plusieurs vulnérabilités dans Apple iOS permettent à une personne distante malintentionnée d'exécuter du code arbitraire et d'élever ses privilèges sur le système.

## 4 Description

Plusieurs vulnérabilités ont été découvertes dans Apple iOS :

- deux vulnérabilités dans la gestion de certaines polices de caractères *FreeType* permettent à une personne distante malintentionnée d'exécuter du code arbitraire via un fichier PDF spécialement conçu (CVE-2010-3855 et CVE-2011-0226) ;
- une erreur de conversion dans l'utilisation de primitives de gestion de queue d'*IOMobileFrameBuffer* permet à une personne malintentionnée d'élever ses privilèges sur le système vulnérable (CVE-2011-0227).

## 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 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

18 juillet 2011 version initiale.