

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-412>

---

### Gestion du document

Référence	CERTA-2011-AVI-412
Titre	Vulnérabilité dans Apple iOS
Date de la première version	26 juillet 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité Apple HT4824 et HT4825 du 25 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

- Atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Apple iOS versions 4.2.5 à 4.2.9 pour iPhone 4 modèle CDMA ;
- Apple iOS versions 3.0 à 4.3.4 pour iPhone 3GS et iPhone 4 modèle GSM ;
- Apple iOS versions 3.1 à 4.3.4 pour iPod touch de 3ème génération et postérieures ;
- Apple iOS versions 3.2 à 4.3.4 pour iPad.

## 3 Résumé

Une vulnérabilité dans Apple iOS a été corrigée et permet à une personne malintentionnée de porter atteinte à l'intégrité et à la confidentialité des données envoyées sur le réseau lors d'une session SSL/TLS.

## 4 Description

Une vulnérabilité dans Apple iOS liée à la validation de la chaîne des certificats X.509 a été corrigée. Elle permet à un utilisateur malintentionné d'utiliser un certificat X.509 spécialement conçu afin d'intercepter le trafic réseau lors d'une session SSL/TLS (attaque de type «*man in the middle*»).

## 5 Solution

Se référer aux bulletins de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Apple HT4824 du 25 juillet 2011 :  
<http://support.apple.com/kb/HT4824>
- Bulletin de sécurité Apple HT4825 du 25 juillet 2011 :  
<http://support.apple.com/kb/HT4825>
- Référence CVE CVE-2011-0228 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0228>

## Gestion détaillée du document

26 juillet 2011 version initiale.