

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'OS iPhone d'Apple

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-2009-AVI-307>

Gestion du document

Référence	CERTA-2009-AVI-307
Titre	Vulnérabilité de l'OS iPhone d'Apple
Date de la première version	05 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité KB HT3754 du 31 juillet 2009
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Apple iPhone OS pour les versions antérieures à la 3.0.1.

3 Résumé

Une vulnérabilité a été identifiée dans la gestion téléphonique du système d'exploitation Apple iPhone OS. Elle peut être exploitée par une personne malveillante distante pour perturber le service de téléphonie ou exécuter des commandes arbitraires.

4 Description

Une vulnérabilité a été identifiée dans la gestion téléphonique du système d'exploitation Apple iPhone OS. Ce dernier ne manipulerait pas correctement les messages au format SMS (*Short Message Service*) qui lui sont destinés (format SMS_DELIVER). La vulnérabilité repose en particulier sur les messages découpés en plusieurs morceaux (qui dépassent donc la limitation de 140 octets ou 160 caractères 7-bits) en jouant sur le nombre de morceaux précisé dans l'en-tête SMS et le nombre de messages partiels réellement envoyés.

Cette vulnérabilité peut être exploitée par une personne malveillante distante pour perturber le service de téléphonie ou exécuter des commandes arbitraires sur l'équipement mobile.

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 HT3754 du 31 juillet 2009 :
<http://support.apple.com/kb/HT3754>
- Référence CVE CVE-2009-2204 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2204>

Gestion détaillée du document

05 août 2009 version initiale.