



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 10 juillet 2009  
N° CERTA-2009-AVI-271

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Apple Safari

---

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-271>

---

### Gestion du document

Référence	CERTA-2009-AVI-271
Titre	Multiples vulnérabilités dans Apple Safari
Date de la première version	10 juillet 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT3666 du 8 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 ;
- injection de code indirecte.

## 2 Systèmes affectés

Safari 4 pour Windows et Mac OS X.

## 3 Résumé

Deux vulnérabilités permettant, entre autre, l'exécution de code arbitraire à distance ont été corrigées.

## 4 Description

Deux vulnérabilités ont été corrigées. La première intervient lors du traitement des objets `parent` et `top` et la seconde lors du traitement de références numériques à des caractères. Une personne malveillante peut utiliser la première pour conduire une attaque en XSS et la seconde pour exécuter du code arbitraire à distance, dans les deux cas, au moyen d'une page web spécialement écrite.

## **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 HT3666 du 08 juillet 2009 :  
<http://support.apple.com/kb/HT3666>
- Référence CVE CVE-2009-1724 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1724>
- Référence CVE CVE-2009-1725 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1725>

## **Gestion détaillée du document**

**10 juillet 2009** version initiale.