

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2012-AVI-141>

Gestion du document

Référence	CERTA-2012-AVI-141
Titre	Multiples vulnérabilités dans Safari
Date de la première version	14 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT5190 du 12 mars 2012
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 ;
- injection de code indirecte à distance.

2 Systèmes affectés

Safari pour Mac OS et Windows versions antérieures à 5.1.4.

3 Résumé

De très nombreuses vulnérabilités ont été corrigées dans Safari, pour de nombreux impacts dont l'exécution de code arbitraire à distance.

4 Description

De très nombreuses vulnérabilités ont été corrigées dans le navigateur Safari :

- de multiples problèmes de corruption mémoire permettent à un attaquant d'exécuter du code arbitraire sur le client à l'aide de pages Web spécialement conçues ;
- l'affichage des caractères dans la barre d'adresse permet de tromper un utilisateur sur l'identité du site qu'il visite ;
- certaines informations sur l'historique des pages visitées sont enregistrées même quand l'option 'Navigation privée' est activée ;
- plusieurs vulnérabilités permettent une injection de code indirecte à distance;
- des cookies peuvent être révélés à un site illégitime.

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 HT5190 du 12 mars 2012 :
<http://support.apple.com/kb/HT5190>
- Référence CVE CVE-2011-2825 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2825>
- Référence CVE CVE-2011-2833 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2833>
- Référence CVE CVE-2011-2846 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2846>
- Référence CVE CVE-2011-2847 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2847>
- Référence CVE CVE-2011-2854 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2854>
- Référence CVE CVE-2011-2855 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2855>
- Référence CVE CVE-2011-2857 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2857>
- Référence CVE CVE-2011-2860 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2860>
- Référence CVE CVE-2011-2866 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2866>
- Référence CVE CVE-2011-2867 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2867>
- Référence CVE CVE-2011-2868 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2868>
- Référence CVE CVE-2011-2869 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2869>
- Référence CVE CVE-2011-2870 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2870>
- Référence CVE CVE-2011-2871 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2871>
- Référence CVE CVE-2011-2872 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2872>
- Référence CVE CVE-2011-2873 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2873>

- Référence CVE CVE-2011-2877 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2877>
- Référence CVE CVE-2011-3881 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3881>
- Référence CVE CVE-2011-3885 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3885>
- Référence CVE CVE-2011-3887 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3887>
- Référence CVE CVE-2011-3888 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3888>
- Référence CVE CVE-2011-3897 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3897>
- Référence CVE CVE-2011-3908 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3908>
- Référence CVE CVE-2011-3909 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3909>
- Référence CVE CVE-2011-3928 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3928>
- Référence CVE CVE-2012-0584 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0584>
- Référence CVE CVE-2012-0585 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0585>
- Référence CVE CVE-2012-0586 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0586>
- Référence CVE CVE-2012-0587 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0587>
- Référence CVE CVE-2012-0588 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0588>
- Référence CVE CVE-2012-0589 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0589>
- Référence CVE CVE-2012-0590 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0590>
- Référence CVE CVE-2012-0591 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0591>
- Référence CVE CVE-2012-0592 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0592>
- Référence CVE CVE-2012-0593 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0593>
- Référence CVE CVE-2012-0594 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0594>
- Référence CVE CVE-2012-0595 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0595>
- Référence CVE CVE-2012-0596 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0596>
- Référence CVE CVE-2012-0597 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0597>
- Référence CVE CVE-2012-0598 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0598>
- Référence CVE CVE-2012-0599 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0599>
- Référence CVE CVE-2012-0600 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0600>

- Référence CVE CVE-2012-0627 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0627>
- Référence CVE CVE-2012-0628 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0628>
- Référence CVE CVE-2012-0629 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0629>
- Référence CVE CVE-2012-0630 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0630>
- Référence CVE CVE-2012-0631 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0631>
- Référence CVE CVE-2012-0632 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0632>
- Référence CVE CVE-2012-0633 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0633>
- Référence CVE CVE-2012-0635 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0635>
- Référence CVE CVE-2012-0636 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0636>
- Référence CVE CVE-2012-0637 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0637>
- Référence CVE CVE-2012-0638 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0638>
- Référence CVE CVE-2012-0639 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0639>
- Référence CVE CVE-2012-0640 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0640>
- Référence CVE CVE-2012-0647 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0647>
- Référence CVE CVE-2012-0648 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0648>

Gestion détaillée du document

14 mars 2012 version initiale.