

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de 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-333>

Gestion du document

Référence	CERTA-2009-AVI-333
Titre	Vulnérabilités de Safari
Date de la première version	12 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT3733 du 11 août 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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Safari 4.x pour Windows et Mac OS X.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans Safari. Certaines d'entre elles permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance sur un système vulnérable.

4 Description

Plusieurs vulnérabilités ont été découvertes dans Safari :

- un débordement de zone mémoire affecte le traitement de certaines chaînes de caractères. Il est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance ;

- un débordement de zone mémoire affecte le traitement de métadonnées EXIF. Il est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance ;
- un débordement de zone mémoire affecte le traitement de l'entrée des nombres en virgule flottante. Il est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance ;
- le support des noms de domaines étendus (avec lettres accentuées, etc.) est utilisable par un utilisateur malveillant pour tromper l'utilisateur sur l'identité réelle du serveur sur lequel il est connecté ;
- la gestion des greffons (*plug-in*) de type inconnu permet à un utilisateur malveillant d'accéder à des informations sensibles ;
- la gestion de l'aperçu des sites favoris peut faciliter les actions de filoutage.

5 Solution

La version Safari 4.0.3 remédie à ces vulnérabilités. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple HT3733 du 11 août 2009 :
<http://support.apple.com/kb/HT3733>
- Référence CVE CVE-2009-2188 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2188>
- Référence CVE CVE-2009-2195 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2195>
- Référence CVE CVE-2009-2196 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2196>
- Référence CVE CVE-2009-2199 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2199>
- Référence CVE CVE-2009-2200 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2200>
- Référence CVE CVE-2009-2468 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2468>

Gestion détaillée du document

12 août 2009 version initiale.