



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 novembre 2008
N° CERTA-2008-AVI-557

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-2008-AVI-557>

Gestion du document

Référence	CERTA-2008-AVI-557
Titre	Vulnérabilités de Safari
Date de la première version	14 novembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT3298 du 13 novembre 2008
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Safari 3.x.

3 Résumé

Plusieurs vulnérabilités affectent le navigateur Safari. Leur exploitation permet d'accéder à des données sensibles ou d'exécuter du code arbitraire à distance sur le système vulnérable.

4 Description

Plusieurs vulnérabilités affectent le traitement des images, en particulier au format PNG, TIFF ou JPEG. L'exploitation de chacune d'entre elles permet d'exécuter du code arbitraire à distance.

Une vulnérabilité dans le traitement des feuilles de style est utilisable de manière malveillante pour exécuter du code arbitraire à distance.

Une vulnérabilité dans le traitement des *javascripts* est utilisable de manière malveillante pour exécuter du code arbitraire à distance.

Une erreur dans *Webkit* et une erreur dans la gestion des formulaires permettent à un utilisateur malveillant d'accéder à des données sensibles.

5 Solution

La version 3.2 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 HT3298 du 13 novembre 2008 :
<http://support.apple.com/kb/HT3298>
- Référence CVE CVE-2005-2096 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2096>
- Référence CVE CVE-2008-1767 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1767>
- Référence CVE CVE-2008-2303 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2303>
- Référence CVE CVE-2008-2317 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2317>
- Référence CVE CVE-2008-2327 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2327>
- Référence CVE CVE-2008-2332 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2332>
- Référence CVE CVE-2008-3608 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3608>
- Référence CVE CVE-2008-3623 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3623>
- Référence CVE CVE-2008-3642 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3642>
- Référence CVE CVE-2008-3644 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3644>
- Référence CVE CVE-2008-4216 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4216>

Gestion détaillée du document

14 novembre 2008 version initiale.