



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 juin 2009
N° CERTA-2009-AVI-223

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-223>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2009-AVI-223 |
| Titre | Multiples vulnérabilités dans Apple Safari |
| Date de la première version | 10 juin 2009 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Apple HT3613 du 8 juin 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les versions de Safari antérieures à 4.0 pour les systèmes d'exploitation suivants :

- Mac OS X 10.4.x ;
- Mac OS X 10.5.x ;
- Mac OS X Server 10.4.x ;
- Mac OS X Server 10.5.x ;
- Windows XP ;
- Windows Vista.

3 Résumé

De multiples vulnérabilités dans `Apple Safari` permettant, entre autre, l'exécution de code arbitraire à distance ont été corrigées.

4 Description

De multiples vulnérabilités dans `Apple Safari` ont été corrigées dont :

- Des images identifiées comme des fichiers `HTML` permettent l'exécution automatique de Javascript ;
- plusieurs corruptions mémoire affectant le composant `CoreGraphics` permettent l'exécution de code arbitraire (`Microsoft Windows`) à distance ;
- plusieurs vulnérabilités affectent le composant `WebKit` et permettent, entre autre, des attaques en XSS ou l'exécution de code arbitraire à distance.

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 HT3613 du 08 juin 2009 :
<http://support.apple.com/kb/HT3613>
- Référence CVE CVE-2006-2783 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2783>
- Référence CVE CVE-2008-1588 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1588>
- Référence CVE CVE-2008-2320 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2320>
- Référence CVE CVE-2008-2321 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2321>
- Référence CVE CVE-2008-3281 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3281>
- Référence CVE CVE-2008-3529 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3529>
- Référence CVE CVE-2008-3632 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3632>
- Référence CVE CVE-2008-4225 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4225>
- Référence CVE CVE-2008-4226 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4226>
- Référence CVE CVE-2008-4231 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4231>
- Référence CVE CVE-2008-4409 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4409>
- Référence CVE CVE-2009-0040 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0040>
- Référence CVE CVE-2009-0145 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0145>
- Référence CVE CVE-2009-0153 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0153>
- Référence CVE CVE-2009-0946 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0946>

- Référence CVE CVE-2009-1179 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1179>
- Référence CVE CVE-2009-1681 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1681>
- Référence CVE CVE-2009-1682 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1682>
- Référence CVE CVE-2009-1684 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1684>
- Référence CVE CVE-2009-1685 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1685>
- Référence CVE CVE-2009-1686 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1686>
- Référence CVE CVE-2009-1687 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1687>
- Référence CVE CVE-2009-1688 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1688>
- Référence CVE CVE-2009-1689 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1689>
- Référence CVE CVE-2009-1690 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1690>
- Référence CVE CVE-2009-1691 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1691>
- Référence CVE CVE-2009-1693 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1693>
- Référence CVE CVE-2009-1694 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1694>
- Référence CVE CVE-2009-1695 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1695>
- Référence CVE CVE-2009-1696 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1696>
- Référence CVE CVE-2009-1697 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1697>
- Référence CVE CVE-2009-1698 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1698>
- Référence CVE CVE-2009-1699 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1699>
- Référence CVE CVE-2009-1700 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1700>
- Référence CVE CVE-2009-1701 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1701>
- Référence CVE CVE-2009-1702 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1702>
- Référence CVE CVE-2009-1703 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1703>
- Référence CVE CVE-2009-1704 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1704>
- Référence CVE CVE-2009-1705 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1705>
- Référence CVE CVE-2009-1706 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1706>
- Référence CVE CVE-2009-1707 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1707>

- Référence CVE CVE-2009-1708 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1708>
- Référence CVE CVE-2009-1709 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1709>
- Référence CVE CVE-2009-1710 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1710>
- Référence CVE CVE-2009-1711 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1711>
- Référence CVE CVE-2009-1712 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1712>
- Référence CVE CVE-2009-1713 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1713>
- Référence CVE CVE-2009-1714 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1714>
- Référence CVE CVE-2009-1715 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1715>
- Référence CVE CVE-2009-1716 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1716>
- Référence CVE CVE-2009-1718 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1718>

Gestion détaillée du document

10 juin 2009 version initiale.