Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 mars 2008
N° CERTA-2008-AVI-145

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Safari

Gestion du document

Référence	CERTA-2008-AVI-145
Titre	Multiples vulnérabilités dans Safari
Date de la première version	19 mars 2008
Date de la dernière version	–
Source(s)	Bulletin de scurité de Apple 307563 du 17 mars 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 ;
- contournement de la politique de sécurité ;
- injection de code indirecte ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Safari 3.0 et les versions antérieures.

3 Résumé

Plusieurs vulnérabilités permettant entre autres des attaques de type injection de code indirecte ou exécution de code arbitraire ont été corrigées dans Safari.

4 Description

La version 3.1 de Safari corrige plusieurs vulnérabilités affectant le navigateur d'`Apple`. Elles permettent de réaliser des attaques d'injection de code indirecte via un site malicieusement construit contenant du *javascript*. Elles permettent aussi d'exécuter du code arbitraire via l'utilisation d'une expression régulière *javascript* spécifiquement réalisée.

5 Solution

Se référer au bulletin de sécurité de Apple 307563 du 17 mars 2008 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple 307563 du 17 mars 2008 :
  http://docs.info.apple.com/article.html?artnum=307563
- Référence CVE CVE-2007-4680 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4680
- Référence CVE CVE-2008-0050 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0050
- Référence CVE CVE-2008-1007 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1007
- Référence CVE CVE-2008-1002 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1002
- Référence CVE CVE-2008-1003 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1003
- Référence CVE CVE-2008-1004 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1004
- Référence CVE CVE-2008-1005 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1005
- Référence CVE CVE-2008-1006 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1006
- Référence CVE CVE-2008-1007 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1007
- Référence CVE CVE-2008-1008 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1008
- Référence CVE CVE-2008-1009 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1009
- Référence CVE CVE-2008-1010 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1010
- Référence CVE CVE-2008-1011 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1011

Gestion détaillée du document

19 mars 2008 version initiale.