Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 juillet 2008
N° CERTA-2008-AVI-331-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du navigateur Safari

Gestion du document

Référence	CERTA-2008-AVI-331-001
Titre	Vulnérabilité du navigateur Safari
Date de la première version	20 juin 2008
Date de la dernière version	04 juillet 2008
Source(s)	Bulletin de sécurité Apple HT2092 du 19 juin 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.

2 Systèmes affectés

- Safari version 3.1.1 pour Windows et versions antérieures ;
- Safari version 3.1.1. pour MacOS et versions antérieures.

3 Résumé

Des vulnérabilités ont été découvertes dans la navigateur `Safari`. Ces vulnérabilités permettent un contournement de la politique de sécurité et l'exécution de code arbitraire à distance sous `Windows`.

4 Description

Une vulnérabilité a été découverte dans la navigateur `Safari` d'`Apple`. Cette vulnérabilité permet via un site spécialement construit de forcer le téléchargement d'un fichier quelconque sur l'ordinateur de la victime. Ce

fichier est téléchargé directement dans le répertoire de téléchargement défini dans les propriétés du navigateur (le Bureau par défaut).

Comme indiqué dans le bulletin d'actualité CERTA-2008-ACT-023, cette vulnérabilité peut également permettre l'exécution de code arbitraire sous Microsoft Windows. En effet, une « fonctionnalité » de Internet Explorer est de charger sous certaines conditions des bibliothèques de fonctions (DLL) depuis le bureau. Le téléchargement d'un tel fichier sous Safari suivi de l'exécution de Internet Explorer permet ainsi à une personne malveillante d'exécuter du code arbitraire à distance.

De plus, une autre vulnérabilité a été découverte dans la manière de traiter les fichiers BMP et GIF par Safari sous Microsoft Windows. Cette vulnérabilité peut être utilisée afin de lire certaines zones de la mémoire.

Une dernière vulnérabilité sur Windows et MacOS concerne un problème de corruption de mémoire dans le traitement de tableaux en Javascript par Webkit. Une personne malintentionnée pourrait exploiter cette faille pour exécuter du code arbitraire à distance.

5 Solution

Se référer aux bulletins de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple HT2092 du 19 juin 2008 :
  http://support.apple.com/kb/HT2092
- Bulletin de sécurité Apple HT2165 du 30 juin 2008 :
  http://support.apple.com/kb/HT2165
- Document du CERTA CERTA-2008-ALE-008 du 20 juin 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-008/index.html
- Référence CVE CVE-2008-1573 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1573
- Référence CVE CVE-2008-2306 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2306
- Référence CVE CVE-2008-2307 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2307

Gestion détaillée du document

20 juin 2008 version initiale.
04 juillet 2008 ajout d'une référence au bulletin d'Apple sur MacOS et mise à jour de la description.