Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 juin 2008
N° CERTA-2008-ALE-008-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité du navigateur Safari

Gestion du document

Référence	CERTA-2008-ALE-008-002
Titre	Vulnérabilité du navigateur Safari
Date de la première version	02 juin 2008
Date de la dernière version	20 juin 2008
Source(s)	Bulletin de sécurité Secunia SA30467 du 02 juin 2008 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

- Contournement de la politique de sécurité ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

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

3 Résumé

Une vulnérabilité a été découverte dans la navigateur `Safari`. Cette vulnérabilité permet 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.

5 Contournement provisoire

Il est préférable généralement de modifier la configuration par défaut des navigateurs, y compris pour Safari :

- changer le répertoire de téléchargement (le `Bureau` par défaut);
- décocher l'option `Ouvrir automatiquement les fichiers fiables` dans les préférences générales ;
- décocher préventivement l'activation de modules externes, ainsi que l'interprétation de Java et de Javascript.

Une autre pratique consiste à filter via un serveur mandataire les champs « Content-Type » et les restreindre à ceux jugés légitimes.

6 Solution

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

7 Documentation

- Bulletin de sécurité Apple HT2092 du 19 juin 2008 :
  http://support.apple.com/kb/HT2092
- Bulletin de sécurité Microsoft 953818 du 30 mai 2008 :
  http://www.microsoft.com/france/technet/security/advisory/953818.mspx
- Bloc-notes de Microsoft du 30 mai 2008 :
  http://blogs.technet.com/msrc/archive/2008/05/30/security-advisory-953818-posted.aspx
- Publication préliminaire sur un bloc-notes Technet Microsoft de R. Hensing le 22 mai 2008 :
  http://blogs.technet.com/robert_hensing/archive/2008/05/22/safari-carpet-bombing-fail-open-goat-award.aspx
- Bulletin d'actualité CERTA-2008-ACT-023 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-023.pdf
- Avis du CERTA CERTA-2008-AVI-331 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-331/index.html

Gestion détaillée du document

02 juin 2008 version initiale ;
09 juin 2008 ajout du risque lié à l'utilisation de Internet Explorer couplé à Safari.
20 juin 2008 correction de l'alerte.