

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-2008-AVI-211>

Gestion du document

Référence	CERTA-2008-AVI-211
Titre	Multiples vulnérabilités dans Apple Safari
Date de la première version	17 avril 2008
Date de la dernière version	–
Source(s)	Article de la base de connaissances Apple HT1467
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- injection de code indirecte.

2 Systèmes affectés

Safari versions antérieures à 3.1.1.

3 Résumé

De multiples vulnérabilités sur *Safari* permettent à une personne malintentionnée distante d'exécuter du code arbitraire, d'effectuer un déni de service, de contourner la politique de sécurité ou d'effectuer une injection de code indirecte.

4 Description

Quatre vulnérabilités ont été identifiées dans le navigateur *Safari* :

- le contenu de la barre d'adresses d'une victime peut être changé sans que la page correspondante soit chargée (CVE-2007-2398) ;
- une erreur de corruption de mémoire pourrait permettre à une personne malintentionnée distante d'exécuter du code arbitraire en incitant une victime à télécharger un fichier ayant un nom spécialement construit (CVE-2008-1024) ;
- un mauvais traitement de certaines URL par *Webkit* permet à une personne malintentionnée d'effectuer des attaques de type injection de code indirecte (*cross-site scripting*) (CVE-2008-1025) ;
- un débordement de mémoire dans le traitement d'expressions régulières en *Javascript* par *Webkit* peut permettre à une personne malintentionnée d'exécuter du code arbitraire à distance (CVE-2008-1026).

Les deux premières vulnérabilités affectent *Safari* sur *Microsoft Windows* uniquement. Les deux suivantes affectent également *Safari* sur *Mac OSX*.

5 Solution

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

6 Documentation

- Article HT1467 de la base de connaissances d'Apple :
<http://support.apple.com/kb/HT1467>
- Référence CVE CVE-2007-2398
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2398>
- Référence CVE CVE-2008-1024
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1024>
- Référence CVE CVE-2008-1025
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1025>
- Référence CVE CVE-2008-1026
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1026>

Gestion détaillée du document

17 avril 2008 version initiale.