



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 mai 2010
N° CERTA-2010-ALE-006-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité de 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-2010-ALE-006>

Gestion du document

Référence	CERTA-2010-ALE-006-001
Titre	Vulnérabilité de Safari
Date de la première version	14 mai 2010
Date de la dernière version	27 mai 2010
Source(s)	–
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

- Déni de service à distance ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Safari 4.0.5 pour Microsoft Windows.

3 Résumé

Une vulnérabilité non-corrigée dans *Safari* permet à un utilisateur distant malintentionné de provoquer un déni de service ou, potentiellement, d'exécuter du code arbitraire.

4 Description

Une vulnérabilité non-corrigée relative à la gestion des fenêtres est présente dans le navigateur *Safari* de *Apple*. Celle-ci est due à la façon dont *Safari* gère la fermeture des fenêtres de type *pop-up* et permet à un utilisateur distant malintentionné de provoquer un déni de service de l'application vulnérable ou d'exécuter du code arbitraire.

Remarque n°1 :

Pour que l'exploitation de la vulnérabilité fonctionne, il est nécessaire que l'option *Bloquer les fenêtres surgissantes* soit désactivée. Ceci n'est pas le cas dans la configuration par défaut du navigateur.

Remarque n°2 :

La vulnérabilité est confirmée pour la version 4.0.5 sous *Microsoft Windows* mais, compte tenu sa nature, il est possible que la version pour *Mac OS X* soit également concernée.

5 Contournement provisoire

Dans l'attente d'un correctif de l'éditeur, le CERTA recommande les mesures suivantes :

- conserver ou réactiver le blocage des fenêtres surgissantes (*Crtl+Maj+K*) ;
- désactiver par défaut le support du *javascript* : Préférences -> Sécurité -> Activer JavaScript ;
- utiliser un navigateur alternatif.

6 Documentation

- Référence CVE CVE-2010-1939 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1939>

Gestion détaillée du document

14 mai 2010 version initiale.

27 mai 2010 ajout de la référence CVE.