

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans le traitement de certains fichiers sous MAC OS X

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-2006-ALE-001>

Gestion du document

Référence	CERTA-2006-ALE-001-001
Titre	Vulnérabilité dans le traitement de certains fichiers sous MAC OS X
Date de la première version	22 février 2006
Date de la dernière version	02 mars 2006
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Apple Mac OS X version 10.4.5 et versions antérieures.

3 Résumé

Une vulnérabilité présente dans le traitement de certains fichiers peut être utilisée par un utilisateur mal intentionné pour exécuter du code arbitraire sur le système.

4 Description

Une vulnérabilité est présente lors de l'ouverture de certains fichiers sous Mac OS X. Cette vulnérabilité associée à la fonctionnalité d'ouverture des pièces jointes après le téléchargement sur le navigateur Safari et sur le client de messagerie Mail peut être exploitée par un utilisateur mal intentionné pour exécuter du code arbitraire à distance.

Deux exemples d'exploitation de cette vulnérabilité sont déjà utilisés :

- Un utilisateur mal intentionné peut exploiter cette vulnérabilité par le biais d'un message ayant un fichier joint de type MIME malicieusement construit envoyé à un destinataire utilisant le client de messagerie Mail d'Apple ;
- un fichier malicieusement construit placé dans une archive compressée au format ZIP récupérée par Safari est un autre moyen d'exploiter la vulnérabilité.

5 Contournement provisoire

Dans l'attente d'un correctif, pour les deux modes d'exploitation cités dans le paragraphe description, il est recommandé aux utilisateurs d'appliquer l'un des contournements provisoires :

- Désactiver la fonction `Open safe files after downloading` dans la section préférences «Général» du navigateur Safari et du client de messagerie Mail ;
- Utiliser un navigateur et client de messagerie alternatifs.

6 Solution

La vulnérabilité a été corrigée, pour plus de détail voir le bulletin de sécurité CERTA-2006-AVI-096

7 Documentation

- Bulletin de sécurité du SANS :
<http://isc.sans.org/diary.php?storyid=1138>
- Bulletin de sécurité Apple du 02 mars 2006 :
<http://docs.info.apple.com/article.html?artnum=108009>
- Bulletin de sécurité CERTA-2006-AVI-096 du 02 mars 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-096/>

Gestion détaillée du document

22 février 2006 version initiale.

02 mars 2006 ajout de la référence à la mise à jour de sécurité Apple.