

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Multiples vulnérabilités sous Mac OS X d'Apple

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-004>

Gestion du document

Référence	CERTA-2006-ALE-004-001
Titre	Multiples vulnérabilités sous Mac OS X d'Apple
Date de la première version	22 avril 2006
Date de la dernière version	12 mai 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 ;
- déni de service à distance.

2 Systèmes affectés

- Apple Mac OS X 10.4.x ;
- Apple Mac OS X 10.3.x.

3 Résumé

De nombreuses vulnérabilités affectant le système d'exploitation Mac OS X d'Apple viennent d'être publiées sur l'Internet avec des codes de démonstration de faisabilité (Proof of Concept).

4 Description

Ces vulnérabilités affectent de nombreuses applications sous Mac OS X.

Le CERTA a testé ces codes de démonstration sur différentes plates-formes et versions Mac OS X.

L'exécution de ces codes de démonstration permet de provoquer un déni de service sur les applications vulnérables ou, potentiellement, d'exécuter du code arbitraire à distance.

La publication des détails techniques ainsi que la parution de codes de démonstration exploitant ces vulnérabilités sur l'Internet traduisent qu'une exploitation à des fins malveillantes est à craindre dans un avenir proche.

Détails des vulnérabilités :

- une vulnérabilité de type débordement de mémoire présente dans la fonction `BOMStackPop` peut être exploitée au moyen d'une archive `zip` créée de manière malveillante afin de provoquer un déni de service ou, potentiellement, d'exécuter du code arbitraire sur le système vulnérable ;
- plusieurs vulnérabilités dans Safari permettent à un individu de provoquer un déni de service à distance ou, potentiellement, d'exécuter du code arbitraire à distance au moyen d'un site web conçu de façon mal intentionnée ;
- une vulnérabilité de type débordement de mémoire dans la fonction `ReadBMP()` peut être exploitée au moyen d'un fichier `bmp` conçu de manière malveillante ;
- une vulnérabilité de type débordement de mémoire dans la fonction `CFAllocatorAllocate()` peut être exploitée au moyen d'un fichier `gif` conçu de manière malveillante ;
- deux vulnérabilités de type débordement de mémoire dans les fonctions `_cg_TIFFSetField()` et `PredictorVSetField()` peuvent être exploitées au moyen d'un fichier `tiff` conçu de manière malveillante.

5 Contournement provisoire

En attendant la publication des mises à jour de sécurité par Apple, il est recommandé :

- d'utiliser d'un navigateur Internet alternatif comme `Firefox` ou `Opera` ;
- de désactiver dans les options du navigateur le chargement des images ;
- de mettre en quarantaine les archives au format `zip` de source non-sure ;
- de porter une vigilance accrue sur les postes affectés.

6 Solution

Des mises à jour sont disponibles sur le site de l'éditeur (cf. section documentation)

7 Documentation

- Multiples bulletins de sécurité Security Protocols du 19 avril 2006 :
http://www.security-protocols.com/sp_x25-advisory.php
http://www.security-protocols.com/sp_x26-advisory.php
http://www.security-protocols.com/sp_x27-advisory.php
http://www.security-protocols.com/sp_x28-advisory.php
http://www.security-protocols.com/sp_x29-advisory.php
http://www.security-protocols.com/sp_x30-advisory.php
- Bulletin de sécurité du CERTA du 12 mai 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-195/index.html>
- Bulletin de sécurité Apple du 12 mai 2006 :
<http://docs.info.apple.com/article.html?artnum=303737>

Gestion détaillée du document

22 avril 2006 version initiale.

12 mai 2006 ajout des références au bulletin de sécurité Apple et au bulletin de sécurité du CERTA.