

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Multiples vulnérabilités dans Apple iCal

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-ALE-007>

Gestion du document

Référence	CERTA-2008-ALE-007-001
Titre	Multiples vulnérabilités dans Apple iCal
Date de la première version	23 mai 2008
Date de la dernière version	29 mai 2008
Source(s)	Bulletin de sécurité Core Security CORE-2008-0126
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 iCal 3.01, 3.02 sur MacOSX 10.5 à 10.5.2 (x86 et PowerPC).
D'autres versions pourraient être vulnérables.

3 Résumé

Trois vulnérabilités sur *Apple iCal* permettent à une personne malintentionnée distante de réaliser un déni de service ou potentiellement exécuter du code arbitraire.

4 Description

iCal est une application de calendrier disponible par défaut sur MacOSX. Ce logiciel utilise notamment des fichiers portant l'extension `.ics` et un protocole nommé `CalDAV` pour le partage d'événements.

Trois vulnérabilités concernant *iCal* ont récemment été publiées. Deux de ces vulnérabilités sont dues à une mauvaise validation de certains entiers. Une personne malintentionnée peut ainsi réaliser un déni de service en incitant un utilisateur à importer un fichier `.ics` spécialement conçu (CVE-2008-2006) et à effectuer certaines actions spécifiques (double-click sur un événement, par exemple).

La troisième vulnérabilité est également due à une mauvaise validation du format d'un fichier `.ics` et permettrait à une personne malintentionnée d'exécuter du code arbitraire en incitant un utilisateur à importer un fichier `.ics` spécialement conçu et à effectuer certaines actions (CVE-2008-2007).

Pour information, les fichiers `.ics` peuvent être importés automatiquement depuis des serveurs `CalDAV`.

Des preuves de faisabilité ont été diffusées sur l'internet.

Apple a corrigé ces vulnérabilités dans sa mise à jour de sécurité 2008-003 publiée le 28 mai 2008 et détaillée dans l'avis CERTA-2008-AVI-278.

5 Contournement provisoire

Le CERTA préconise les recommandations suivantes :

- n'importer que des fichiers `.ics` provenant de personnes de confiance ;
- ne s'inscrire que sur des serveurs `CalDAV` de confiance ;
- entrer les événements manuellement ;
- dans l'attente d'un correctif, utiliser une application de calendrier alternative.

6 Solution

Le CERTA recommande d'appliquer les correctifs 2008-003 d'Apple publiés le 28 mai 2008 et détaillés dans l'avis CERTA-2008-AVI-278.

7 Documentation

- Avis CERTA-2008-AVI-278 du 28 mai 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-278/>
- Bulletin de sécurité Core Security CORE-2008-0126 :
<http://www.coresecurity.com/index.php5?module=ContentMod&action=item>
- Bulletin du NIST CVE-2008-2007 du 22 mai 2008 :
<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2007>
- Bulletin du NIST CVE-2008-2006 du 22 mai 2008 :
<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2006>

Gestion détaillée du document

23 mai 2008 version initiale.

29 mai 2008 ajout de la référence aux correctifs publiés par Apple et décrits dans CERTA-2008-AVI-278.