

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans la gestion RTSP d'Apple QuickTime

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-2007-ALE-017>

Gestion du document

Référence	CERTA-2007-ALE-017
Titre	Vulnérabilité dans la gestion RTSP d'Apple QuickTime
Date de la première version	27 novembre 2007
Date de la dernière version	14 décembre 2007
Source(s)	Bulletin de sécurité de l'US-CERT VU#659761 du 24 novembre 2007
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

- La version 7.3 d'Apple QuickTime ainsi que les versions antérieures ;
- La version 7.5 d'Apple iTunes ainsi que les versions antérieures.

3 Résumé

Une vulnérabilité a été identifiée dans le logiciel multimédia Apple QuickTime. Ce dernier ne manipule pas correctement un champ dans l'en-tête des réponses retournées par le serveur de flux RTSP. Une personne malveillante pourrait inciter un utilisateur à se rendre sur un tel serveur, ce qui pourrait alors perturber son système ou permettre à l'attaquant d'exécuter des commandes arbitraires.

4 Description

Une vulnérabilité a été identifiée dans le logiciel multimédia Apple QuickTime. Ce dernier ne manipulerait pas correctement un champ dans l'en-tête des réponses retournées par le serveur de flux RTSP.

RTSP (pour *Real Time Streaming Protocol*) est un protocole permettant d'établir et de contrôler des flux synchronisés de médias continus (*streaming*), qu'ils soient audio ou vidéo. Il est conceptuellement très proche de HTTP : il est à état et utilise la notion de session.

Lorsque le client envoie une requête au serveur, ce dernier retourne une réponse, avec un champ `Content-Type`.

Apple QuickTime n'interpréterait pas correctement la valeur de ce champ. Cette vulnérabilité peut ainsi être exploitée par une personne distante, qui aura pris soin de mettre en place un serveur de flux répondant par cette vulnérabilité. L'utilisateur amené à récupérer le flux multimédia, par un lien par exemple provoquera le dysfonctionnement, voire l'exécution de code arbitraire sur son système vulnérable.

5 Contournement provisoire

5.1 De manière générale

Il est préférable, dans l'attente d'un correctif, d'utiliser un lecteur multimédia alternatif.

L'administrateur du réseau peut également vérifier que les flux sortants TCP/UDP vers le port 554 sont bloqués. Ces ports sont ceux par défaut attribués au protocole `Real Time Streaming Protocol`, mais peuvent être changés et remplacés par n'importe quel autre port convenu côté serveur et côté client. Cette mesure n'est donc pas suffisante.

Les navigateurs offrent également la possibilité de désactiver les modules ou *plugins*.

Les recommandations standards s'appliquent toujours : l'interprétation de codes dynamiques comme Javascript doit être désactivée par défaut.

5.2 Sous Microsoft Windows :

- Désactiver la prise en charge des liens `rtsp://` dans Quicktime en décochant la case Préférences de Quicktime -> Types de fichiers -> Diffusion -> Descripteur de flux RTSP;
- Désactiver l'association faite entre le type de fichier et QuickTime, en supprimant les clés de registre de la forme
`HKEY_CLASSES_ROOT\QuickTime.*`

5.3 Sous Apple MacOS X :

- Désactiver la prise en charge des liens `rtsp://` dans QuickTime en décochant la case Préférences de Quicktime -> Avancé -> Réglages MIME -> Diffusion -> Descripteur de flux RTSP;

6 Solution

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

7 Documentation

- Bulletin de sécurité QuickTime du 13 décembre 2007 :
<http://docs.info.apple.com/article.html?artnum=307176>
- Site de téléchargement d'Apple QuickTime :
<http://www.apple.com/quicktime/>
- RFC 2326, "Real Time Streaming Protocol" :
<http://tools.ietf.org/html/rfc2326>
- Note de vulnérabilité de l'US-CERT VU#659761 du 24 novembre 2007 :
<http://www.kb.cert.org/vuls/id/659761>

- Référence CVE CVE-2007-0015 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0015>
- Référence CVE CVE-2007-6166 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6166>
- Alerte CERTA-2007-ALE-001 du 04 janvier 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-001/>
- Désinstaller des modules ou *plugins* sous Mozilla :
<http://plugindoc.mozdev.org/faqs/uninstall.html>

Gestion détaillée du document

27 novembre 2007 version initiale.

14 décembre 2007 ajout de la référence au bulletin de sécurité QuickTime.