*UNAM−CERT*

*Departamento de Seguridad en Cómputo*

*DGSCA−UNAM*

---

# *Boletin de Seguridad UNAM−CERT−2007−009*

## *Actualización de seguridad de QuickTime*

---

Apple QuickTime contiene múltiples vulnerabilidades. La explotación de estas vulnerabilidades permitiría a un intruso ejecutar código arbitrario o provocar una negación de servicio de forma remota.

**Fecha de Liberación**: 6 de Marzo de 2007

**Ultima Revisión**: 6 de Marzo de 2007

**Fuente**: CERT/CC

**CVE ID**: **−2006−1190**

**Riesgo**

Muy Alto

**Problema de Vulnerabilidad**

Remoto

**Tipo de Vulnerabilidad**

Múltiples vulnerabilidades

### I. Sistemas Afectados

Apple QuickTime ejecutándose en sistemas

- Apple Mac OS X
- Microsoft Windows

### II. Descripción

La versión 7.5.1 resuelve múltiples vulnerabilidades relacionadas con el manejo de distintos tipos de archivos de imágenes y multimedia. Un intruso puede explotar estas vulnerabilidades convenciendo a un usuario, que cuente con la versión vulnerable de QuickTime, de acceder a archivos de imágenes y multimedia modificados con fines maliciosos. Debido a que QuickTime puede ser configurado para usarse con navegadores Web, un intruso puede aprovechar esto para diseñar su ataque haciendo uso de un sitio Web.

Es importante mencionar que QuickTime interactúa con Apple iTunes.

Más detalles de esta vulnerabilidad se encuentran disponibles en las notas de vulnerabilidad.

## III. Impacto

Esta vulnerabilidad permite que un intruso pueda, sin previa autenticación, ejecutar código o comandos arbitrarios de forma remota y provocar una negación de servicio.

## IV. Solución

**Actualizar QuickTime**

Actualizar QuickTime a la versión 7.1.5. Esta y otras actualizaciones están disponibles por medio de la herramienta “Actualización de software” de Apple.

Para el sistema Windows de Microsoft, la opción “actualización de software” no detectará una nueva versión disponible. Los usuarios de Windows requerirán descargar la actualización haciendo uso de “Apple Software Update” e instalarlo de forma manual.

**Deshabilitar QuickTime del navegador Web.**

Un intruso podrá diseñar un sitio Web que contenga archivos de imagen y multimedia especialmente modificados para explotar esta vulnerabilidad. Para no ser víctimas de un ataque descargando archivos de un sitio malicioso, es importante desactivar QuickTime del navegador Web. Para más información relacionada con la forma de desactivar la aplicación del navegador Web, referirse a la documentación del navegador de su preferencia.

## V. Referencias

- Vulnerability Notes for QuickTime 7.1.5 − http://www.kb.cert.org/vuls/byid?searchview715
- About the security content of the QuickTime 7.1.5 Update http://docs.info.apple.com/article.html?artnum=305149
- How to tell if Software Update for Windows is working correctly when no updates are available − http://docs.info.apple.com/article.html?artnum=304263
- Apple QuickTime 7.1.5 for Windows − http://www.apple.com/support/downloads/quicktime715forwindows.html
- Apple QuickTime 7.1.5 for Mac − http://www.apple.com/support/downloads/quicktime715formac.html
- Standalone Apple QuickTime Player − http://www.apple.com/quicktime/download/standalone.html
- Mac OS X: Updating your software − http://docs.info.apple.com/article.html?artnum=106704
- Securing Your Web Browser − http://www.us−cert.gov/reading_room/securing_browser/

---

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Israel Becerril Sierra (ibecerril at seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)

---

***UNAM−CERT***
***Equipo de Respuesta a Incidentes UNAM***
***Departamento de Seguridad en Cómputo***
***E−Mail: seguridad@seguridad.unam.mx***
***http://www.cert.org.mx***
***http://www.seguridad.unam.mx***
***ftp://ftp.seguridad.unam.mx***
***Tel: 56 22 81 69***
***Fax: 56 22 80 43***