

UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletín de Seguridad UNAM-CERT-2006-029

Múltiples vulnerabilidades en QuickTime de Apple

El CERT/UNAM-CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo, informan que QuickTime de Apple contiene múltiples vulnerabilidades. La explotación de estas vulnerabilidades podría permitir a un intruso remoto la ejecución de código arbitrario o provocar una condición de negación de servicio.

Fecha de Liberación: 13 de Septiembre de 2006

Última Revisión: 13 de Septiembre de 2006

Fuente: CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Sistemas Afectados

QuickTime	<7.1.3
------------------	--------

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Impacto

Esta vulnerabilidad puede ser explotada de forma remota, no será necesario que un intruso se autentiquen para ejecutar comandos o código arbitrario y con ello causar una negación de servicio (DoS).

II. Descripción

La versión 7.1.3 de Apple QuickTime repara múltiples vulnerabilidades en la manipulación de archivos de imágenes y video. Un intruso puede explotar esta vulnerabilidad al tratar de hacer que el usuario acceda a una imagen o video previamente modificado con una versión de QuickTime vulnerable. Si se tiene configurado QuickTime con el navegador Web para ver videos, un intruso puede aprovechar esta configuración para explotar dicha vulnerabilidad.

Es importante destacar que iTunes hace uso de QuickTime.

III. Solución

Actualizar QuickTime

Actualizar QuickTime a la versión 7.1.3. Tanto ésta como las demás actualizaciones para Mac OS X están disponibles vía Apple Update.

Deshabilitar el uso de QuickTime en el navegador Web

Un intruso puede explotar esta vulnerabilidad al hacer que el usuario acceda a un sitio Web en el que pueda ver videos previamente modificados. Para no ser víctima de este ataque, es importante deshabilitar QuickTime del navegador Web

IV. Referencias

- ◆ Vulnerability Notes for QuickTime 7.1.3 –
<http://www.kb.cert.org/vuls/byid?searchview713>
- ◆ About the security content of the QuickTime 7.1.3 Update –
<http://docs.info.apple.com/article.html?artnum=304357>
- ◆ Apple QuickTime 7.1.3 –
<http://www.apple.com/support/downloads/quicktime713.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 Computo/UNAM-CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

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

UNAM-CERT

Equipo de Respuesta a Incidentes UNAM

Departamento de Seguridad en Computo

E-Mail: seguridad@seguridad.unam.mx

http://www.cert.org.mx

http://www.seguridad.unam.mx

ftp://ftp.seguridad.unam.mx

UNAM-CERT

Tel: 56 22 81 69

Fax: 56 22 80 43