

UNAM-CERT**Departamento de Seguridad en Cómputo****DGSCA-UNAM**

Boletín de Seguridad UNAM-CERT-2006-017

Vulnerabilidades en Apple QuickTime

Apple QuickTime contiene múltiples vulnerabilidades. La explotación de estas vulnerabilidades podría permitir a un intruso remoto ejecutar código arbitrario o causar una condición de negación de servicio.

Fecha de Liberación: 12 de Mayo de 2006

Última Revisión: 12 de Mayo de 2006

Fuente: CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión.

Sistemas Afectados

Microsoft Windows	QuickTime	↵versión 7.1
OS X	QuickTime	↵versión 7.1

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución remota de código y negación de servicio

I. Descripción

Apple QuickTime 7.1 contiene múltiples vulnerabilidades en la forma en que son manejados diferentes tipos de imágenes y archivos multimedia. Un intruso podría explotar estas vulnerabilidades convenciendo a un usuario de que acceda a una imagen o un archivo multimedia creados de forma maliciosa a través de

una versión vulnerable de QuickTime. Debido a que QuickTime configura la mayoría de los navegadores para manejar archivos multimedia de QuickTime, un intruso podría explotar estas vulnerabilidades utilizando una página Web.

Para mayor información, consulte las Notas de Vulnerabilidades asociadas con éste problema.

II. Impacto

El impacto de estas vulnerabilidades podría permitir a un intruso remoto no autenticado ejecutar código o comandos arbitrarios, y causar una condición de negación de servicio. Para mayor información, consulte las Notas de Vulnerabilidades asociadas con éste problema.

III. Solución

◆ Actualizar.

Actualizar a QuickTime 7.1. Esta y otras actualizaciones para Mac OS X están disponibles a través del sitio Apple Update.

◆ Deshabilitar QuickTime en su navegador.

Un intruso podría ser capaz de explotar esta vulnerabilidad persuadiendo a un usuario para que acceda a un archivo creado de forma maliciosa a través de un navegador Web. Deshabilitando QuickTime en su navegador Web lo protegerá contra éste vector de ataque. Para mayor información, consulte el documento Asegurando tu Navegador Web (documento en inglés).

IV. Apéndice A. Referencias

- ◆ Notas de Vulnerabilidad para QuickTime 7.1 –
<http://www.kb.cert.org/vuls/byid?searchview&query=QuickTime_7.1>
- ◆ Asegurando tu navegador Web –
<http://www.us-cert.gov/reading_room/securing_browser/>
- ◆ Acerca del contenido de seguridad de la Actualización QuickTime 7.1 –
<<http://docs.info.apple.com/article.html?artnum=303752>>
- ◆ Apple QuickTime 7.1 –
<<http://www.apple.com/support/downloads/quicktime71.html>>
- ◆ Standalone Apple QuickTime Player –
<<http://www.apple.com/quicktime/download/standalone.html>>
- ◆ Mac OS X: Actualizando tu software –
<<http://docs.info.apple.com/article.html?artnum=106704>>

El Departamento de Seguridad en Computo/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)
- Jesús Ramón Jiménez Rojas (jrojas at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Computo

UNAM-CERT

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