

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

Boletín de Seguridad UNAM-CERT-2006-003

Vulnerabilidades en QuickTime de Apple

El CERT/UNAM-CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo, informan que Apple ha liberado la versión 7.0.4 de QuickTime para corregir varias vulnerabilidades. El impacto de estas vulnerabilidades incluye la ejecución de código arbitrario y negación de servicio.

Fecha de Liberación: 11 de Enero de 2006

Última Revisión: 11 de Enero de 2006

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

Sistemas Afectados

Mac OS X	QuickTime	<7.0.4
Windows 2000	QuickTime	<7.0.4
Windows XP	QuickTime	<7.0.4

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Descripción

La versión 7.0.4 de QuickTime de Apple resuelve varias vulnerabilidades de manejo de imagen y archivos multimedia. Puede encontrarse más información en las siguientes Notas de Vulnerabilidades:

[VU#629845](#) – Buffer overflow en el manejo de imágenes de QuickTime de Apple

QuickTime de Apple contiene una vulnerabilidad de heap overflow que podría permitir a un intruso ejecutar código arbitrario o provocar una condición de negación de servicio. (CAN-2005-2340)

VU#921193 – QuickTime de Apple no maneja adecuadamente los archivos multimedia corruptos.

QuickTime de Apple contiene una vulnerabilidad de heap overflow en el manejo de archivos multimedia. Esta vulnerabilidad podría permitir a un intruso remoto, no autenticado, ejecutar código arbitrario o provocar una negación de servicio en un sistema vulnerable. (CAN-2005-4092)

VU#115729 – QuickTime de Apple no maneja adecuadamente las imágenes TGA corruptas.

Una falla en la forma en que QuickTime de Apple maneja los archivos de formato de imagen Targa (TGA) podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable. (CAN-2005-3707)

VU#150753 – QuickTime de Apple no maneja adecuadamente las imágenes TIFF corruptas

QuickTime de Apple contiene una vulnerabilidad de desbordamiento de entero en el manejo de imágenes TIFF. Esta vulnerabilidad podría permitir a un intruso remoto, no autenticado ejecutar código arbitrario o provocar una negación de servicio en un sistema vulnerable. (CAN-2005-3710)

VU#913449 – QuickTime de Apple no maneja adecuadamente las imágenes Gif corruptas

Una falla en la forma en que QuickTime de Apple maneja los archivos Graphics Interchange Format (GIF) podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable. (CAN-2005-3713)

Puede ver una descripción de todas las vulnerabilidades en español en el siguiente enlace:

<<http://www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=4991>>

II. Impacto

Los impactos de estas vulnerabilidades varían. Para información sobre impactos específicos, ver las Notas de Vulnerabilidades. Las consecuencias potenciales incluyen la ejecución remota de código arbitrario o comandos y negación de servicio.

III. Solución

Actualizar

Actualizar a QuickTime 7.0.4

IV. Apéndice A. Referencias

- ◆ Nota de Vulnerabilidad del US-CERT VU#629845 –
<<http://www.kb.cert.org/vuls/id/629845>>
- ◆ Nota de Vulnerabilidad del US-CERT VU#921193 –
<<http://www.kb.cert.org/vuls/id/921193>>
- ◆ Nota de Vulnerabilidad del US-CERT VU#115729 –

UNAM-CERT

- <<http://www.kb.cert.org/vuls/id/115729>>
 - ◆ Nota de Vulnerabilidad del US-CERT VU#150753 –
<<http://www.kb.cert.org/vuls/id/150753>>
 - ◆ Nota de Vulnerabilidad del US-CERT VU#913449 –
<<http://www.kb.cert.org/vuls/id/913449>>
 - ◆ CVE-2005-2340 –
<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2340>>
 - ◆ CVE-2005-4092 –
<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4092>>
 - ◆ CVE-2005-3707 –
<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3707>>
 - ◆ CVE-2005-3710 –
<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3710>>
 - ◆ CVE-2005-3713 –
<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3713>>
 - ◆ Contenido de seguridad de QuickTime 7.0.4 –
<<http://docs.info.apple.com/article.html?artnum=303101>>
 - ◆ QuickTime 7.0.4 –
<<http://www.apple.com/support/downloads/quicktime704.html>>
 - ◆ Actualización Mac OS X 10.4.4 (Delta)–
<<http://docs.info.apple.com/article.html?artnum=302810>>
-

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

- Ruben Aquino Luna (raquno at seguridad dot unam dot mx)
 - David Jiménez Domínguez (djimenez at correo dot 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