UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−020

Actualización de Apple para múltiples vulnerabilidades en QuickTime

---

Apple QuickTime presenta múltiples vulnerabilidades. Éstas vulneraibilidades permiten que un intruso de forma remota ejecute código arbitrario o provoque una negación de servicio.

Fecha de Liberación: 12 de Julio de 2007

Ultima Revisión: 12 de Julio de 2007

Fuente: CERT/CC

CVE ID: **2007−020**

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. **Descripción**

Apple QuickTime presenta multiples vulnerabilidades en la forma en la que manipula los applets de JAVA y varios tipos de archivos multimedia. Los intrusos pueden aprovechar estas vulnerabilidades haciendo que los usuarios accedan a archivos multimedia o applets de JAVA especialmente modificados con la versión de Apple Quicktime vulnerable. También es posible crear una página Web que haga uso de archivos multimedia especialmente modificados para el ataque, el intruso sólo necesitaría que sus víctimas visiten dicho sitio.

II. **Impacto**

Estas vulnerabilidades podrían permitir una negación de servicio o la ejecución de código o comandos arbitrarios de forma remota y sin necesidad de autenticarse. Para más referencia, consultar la base de datos de notas referentes a la vulnerabilidad.

III. Solución

- Actualizar QuickTime

  Actualizar QuickTime a la versión 7.2. Ésta y otras actualizaciones de Mac OS X, se encuentran disponibles por medio Apple Update.

  En el caso de Microsoft Windows, los usuarios podrán actualizar QuickTime con la herramienta de actualización automática, Apple Software Update, o instalando la actualización de forma manual.

- Deshabilitar QuickTime del navegador Web.

  Un intruso puede aprovechar la interacción que tiene QuickTime con los navegadores Web para explotar dicha vulnerabilidad. Para que un intruso tenga éxito en su ataque, basta con crear un sitio Web malicioso. Deshabilitar la interacción de QuickTime con el navegador Web reduce el riesgo en este vector de ataque. Para más referencia, consultar las notas de la vulnerabilidad que Apple publica.

- Deshabilitar JAVA del navegador Web.

  Un intruso puede aprovechar la interacción que tiene JAVA con los navegadores Web para explotar dicha vulnerabilidad. Para que un intruso tenga éxito en su ataque, basta con crear un sitio Web malicioso. Deshabilitar la interacción de JAVA con el navegador Web redice el riesgo en este vector de ataque.

IV. Referencias

- Vulnerability Notes for QuickTime 7.2 − http://www.kb.cert.org/vuls/byid?searchview72
- About the security content of the QuickTime 7.2 Update − http://docs.info.apple.com/article.html?artnum=305947
- 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 7.2 for Windows − http://www.apple.com/support/downloads/quicktime72forwindows.html
- Apple QuickTime 7.2 for Mac − http://www.apple.com/support/downloads/quicktime72formac.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