UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−031

Buffer Overflow en RTSP de Apple QuickTime

Apple QuickTime contiene una vulnerabilidad de buffer overflow en la administración de procesos de Real Time Streaming Protocol (RTSP). La explotación de esta vulnerabilidad podría permitir a un intruso ejecutar código arbitrario

Fecha de Liberación:	30 de Noviembre de 2007
Ultima Revisión:	25 de Enero de 2008
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Buffer Overflow

I. Sistemas Afectados

Un buffer overflow en Apple QuickTime afecta a:

- Apple QuickTime para Windows
- Apple QuickTime para Apple Max OS X

II. Descripción

Apple QuickTime contiene una vulnerabilidad de buffer overflow en la forma en la que Quicktime maneja el encabezado Content−Type RTSP. La versión 7.3 y la mayoría de las versiones anteriores de QuickTime son vulnerables, tanto las que se ejecutan en Mac OS X como las se ejecutan en Windows. Esta vulnerabilidad también afecta a iTunes debido a que QuickTime es un componente de iTunes.

Un intruso puede explotar esta vulnerabilidad convenciendo a los usuarios de acceder a documentos HTML especialmente diseñados, como una página o un correo electrónico. El documento HTML diseñado para explotar la vulnerabilidad, podría utilizar diversas técnicas para provocar que QuickTime cargue flujo de RTSP maliciosamente modificado. Pueden usarse navegadores comunes como Microsoft Internet Explorer, Mozilla Firefox o Apple Safari para pasar flujos RTSP a Quicktime, explotar la vulnerabilidad y ejecutar código arbitrario.

El exploit para esta vulnerabilidad fue publicado por primera vez el 25 de Noviembre del 2007.

III. Impacto

Esta vulnerabilidad podría permitir la ejecución remota de código arbitrario o la ejecución de comandos, sin necesidad de autenticarse y provocar una negación de servicio.

IV. Solución

Hasta el 30 de Noviembre del 2007, no hay disponible una actualización de QuickTime para esta vulnerabilidad. Para bloquear vectores de ataque, considere las siguientes soluciones temporales:

Bloquear el protocolo rtsp://

El uso de un servidor proxy o firewall capaz de reconocer y bloquear el tráfico RTSP puede mitigar esta vulnerabilidad. El exploit publicado para explotar esta vulnerabilidad utiliza el puerto 554/tcp, sin embargo, RTSP puede usar diversos puertos.

Deshabilitar la asociación de archivos para QuickTime

Deshabilitar la asociación de archivos configurados para QuickTime. Esto se puede hacer eliminando las siguientes llaves del registro:

HKEY_CLASSES_ROOT\QuickTime.*

Esto eliminará la asociación de aproximadamente 32 diferentes tipos de archivos que pueden ser abiertos con QuickTime Player.

Desactivar los controles ActiveX de Quicktime en Internet Explorer

Los controles ActiveX de Quicktime pueden deshabilitarse en Internet Explorer configurando el kill bit de los siguientes CLSIDs:

{02BF25D5−8C17−4B23−BC80−D3488ABDDC6B}

{4063BE15−3B08−470D−A0D5−B37161CFFD69}

Más información relacionada con el kill bit, se encuentra disponible en el articulo 240797 de Microsoft Knolwedgebase. Tambien puede guardarse la siguiente información en un archivo con extensión .REG e importarlo para

configurar el kill bit para estos controles:

Windows Registry Editor Versión 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX

Compatibility\{02BF25D5−8C17−4B23−BC80−D3488ABDDC6B}]

"Compatibility Flags"=dword:00000400

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX

Compatibility\{4063BE15−3B08−470D−A0D5−B37161CFFD69}]

"Compatibility Flags"=dword:00000400

Deshabilitar el plug−in de QuickTime para navegadores basados en Mozilla

Los usuarios de navegadores basados en Mozilla, como Firefox, pueden deshabilitar el plug−in de QuickTime, tal y como se especifica en el articulo PluginDoc Desinstalando Plug−ins

Deshabilitar JavaScript

Para consultar las instrucciones de cómo deshabilitar JavaScript, consultar el documento "Securing Your Web Browser". Este puede ayudar a prevenir algunas técnicas de ataque que utilizan el plug−in o control ActiveX de QuickTime .

Asegurar el navegador Web

Para ayudar a mitigar esta y otras vulnerabilidades que pueden ser explotadas a través del navegador Web, referirse al documento "Securing Your Web Browser".

No acceder a archivos de QuickTime de fuentes no confiables.

No abrir archivos de QucikTime de fuentes no confiables, incluyendo archivos no solicitados o enlaces recibido en correos electrónicos, foros Web o canales IRC.

V. Referencias

- US−CERT Vulnerability Note VU#659761 − http://www.kb.cert.org/vuls/id/659761
- Securing Your Web Browser − http://www.us−cert.gov/reading_room/securing_browser/
- Mozilla Uninstalling Plugins − < http://plugindoc.mozdev.org/faqs/uninstall.html>

- How to stop an ActiveX control from running in Internet Explorer − ≤ http://support.microsoft.com/kb/240797>
- IETF RFC 2326 Real Time Streaming Protocol − ≤ http://tools.ietf.org/html/rfc2326>

Material

Documento: quicktime_player.pdf (347080kb)

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

- Ruben Aquino Luna (raquino 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 Cómputo
incidentes at seguridad.unam.mx
phishing at 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