UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−002

Buffer overflow en RTSP de Apple QuickTime

Apple QuickTime contiene un buffer overflow en el manejo de URLs RTSP. Esto podría permitir a un atacante remoto ejecutar código arbitrario en un sistema vulnerable.

Fecha de Liberación:	5 de Enero de 2007
Ultima Revisión:	9 de Enero de 2007
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Buffer Overflow

I. Sistemas afectados

Apple QuickTime ejecutándose en sistemas:

- Apple Mac OS X
- Microsoft Windows

Se debe hacer notar que Apple iTunes y otro software utilizando los componentes de QuickTime vulnerables también son afectados.

II. Descripción

Existe una vulnerabilidad en la forma en como Apple QuickTime maneja cadenas URL del tipo RTSP (Real Time Streaming Protocol) creadas de forma maliciosa. Hoy en día existe código de exploit público que demuestra la forma en como al abrir un archivo .QTL se activa un buffer overflow. Sin embargo, se ha confirmado que existen otros vectores de ataque para la vulnerabilidad.

Los posibles vectores de ataques incluyen:

- Una página Web que utiliza el plugin o control ActiveX de QuickTime.
- Una página Web que utilice el protocolo rtsp://
- Un archivo que está asociado con el Reproductor de QuickTime.

El US−CERT está dando seguimiento a éste problema como la Nota de Vulnerabilidad VU#442497. Este número de referencia corresponde al CVE−2007−0015.

Se debe hacer notar que esta vulnerabilidad afecta a QuickTime en Microsoft Windows y plataformas Apple Mac. Aunque las páginas Web pueden ser utilizadas como vectores de ataque, esta vulnerabilidad no depende de que sea empleado un navegador Web específico.

III. Impacto

Convenciendo a un usuario para que abra un contenido de QuickTime creado de forma maliciosa, un atacante remoto no autenticado puede ejecutar código arbitrario en un sistema vulnerable.

IV. Solución

Actualmente no se tiene una solución para este problema. Hasta que una solución llegue a estar disponible, se recomienda aplicar las soluciones temporales proporcionadas en la Nota de Vulnerabilidad VU#442497.

V. Referencias

- Nota de Vulnerabilidad del US−CERT VU#442497 − <http://www.kb.cert.org/vuls/id/442497>
- Asegurando su navegador Web (en inglés) − <http://www.us−cert.gov/reading_room/securing_browser/>
- CVE−2007−0015 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2007−0015>

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

- Jesús Ramón Jiménez Rojas (jrojas 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