Departamento de Seguridad en Cómputo

UNAM-CERT

Buffer-overflow remoto en QuickTime Player

Resumen

QuickTime Player tiene una vulnerabilidad de buffer-overflow cuando maneja las cabeceras de respuesta de RTSP.

Proyecto Análisis de Vulnerabilidades
Elaboró: Vicente Hernández Jiménez
Revisó: Alejandro Nuñez Sandoval

Índice de contenido

1. Antecedentes

Real Time Streaming Protocol (RTSP) es un protocolo usado por los sistemas multimedia de flujo.

Apple QuickTime tiene una vulnerabilidad de "overflow" en la forma en la que maneja el contenido de las cabeceras RTSP. Esta vulnerabilidad puede ser explotada engañando a un usuario para que a se conecte con un flujo RTSP que ha sido manipulado. QuickTime es un componente de Apple iTunes, por lo cuál las instalaciones de iTunes también se ven afectadas por esta vulnerabilidad.

Se ha informado que las versiones de QuickTime 4.0 a la 7.3, son vulnerables en las plataformas Mac y Windows.

2. Exploit

En milw0rm se ha publicado un exploit para esta vulnerabilidad, el cúal esta escrito en python y envía una cabecera manipulada de RTSP (puerto 554 TCP).

2.1 Metodología

Se descargó de [MWQT] el exploit para Windows XP Service Pack 2 y se probó sobre una máquina Windows XP Professional, Service Pack 2 con QuickTime Player 7.2.

2.2 Explotación

QuickTime hace uso de los archivos .qtl, para reproducir los archivos media de manera más accesible. Estos archivos QTL están escritos en XML y contienen información sobre el archivo media que se reproduce.

Se utilizó el siguiente archivo qtl, con el nombre de “prueba.mp3”

```
<?xml version="1.0">
<?quicktime type="application/x-quicktime-media-link"?>
<embed src="rtsp://172.16.27.131" autoplay="true"/>
```

Este archivo puede ponerse como link en un archivo html, y QuickTime reproducirá el archivo utilizando el protocolo RTSP, como se índica en la siguiente línea:

```
<embed src="rtsp://172.16.27.131" autoplay="true"/>
```

En la máquina 172.16.27.131 es donde se tiene ejecutando el exploit, que lo único que hace es escuchar peticiones por el puerto 554 y responder con una cabecera enviando el carácter 'A' repetido 995 veces y el carácter 'B' 4096 veces.

3. Resultados y conclusiones

A la fecha no se ha liberado una solución para esta vulnerabilidad, sin embargo en [CQT] se encuentran “workarounds” que no eliminan la vulnerabilidad, pero bloquean algunos vectores de ataque.

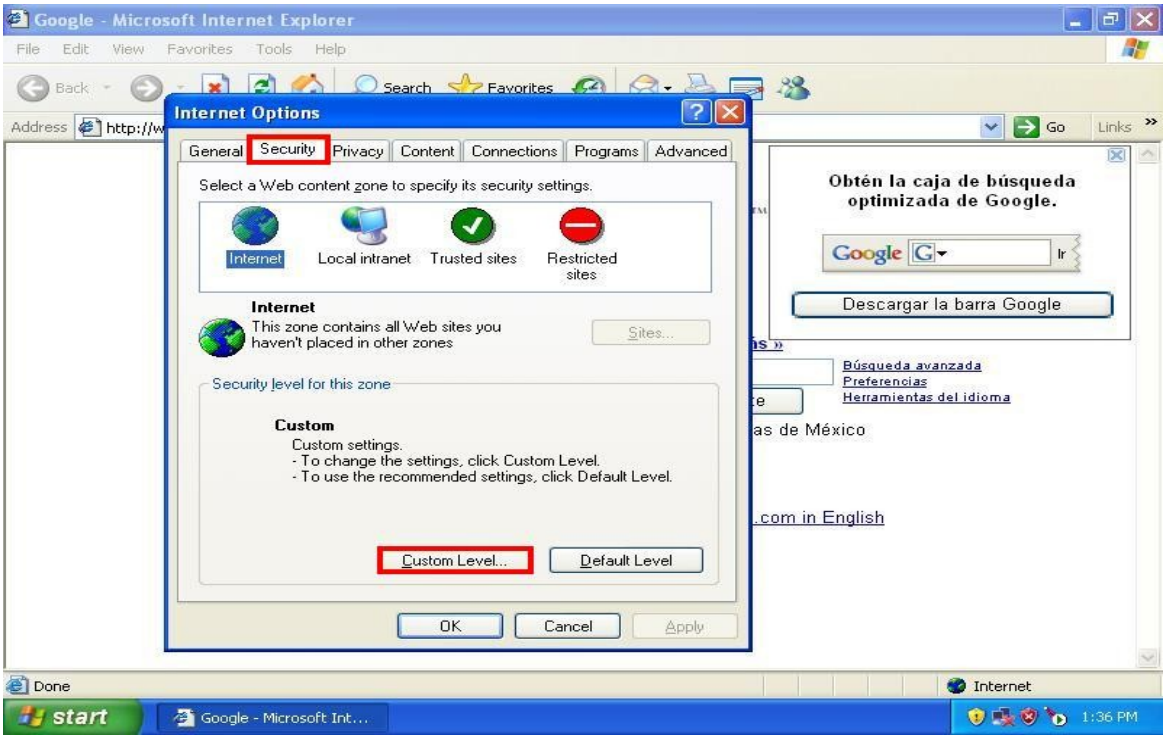
A continuación se muestran los “workaround” que funcionaron durante las pruebas.

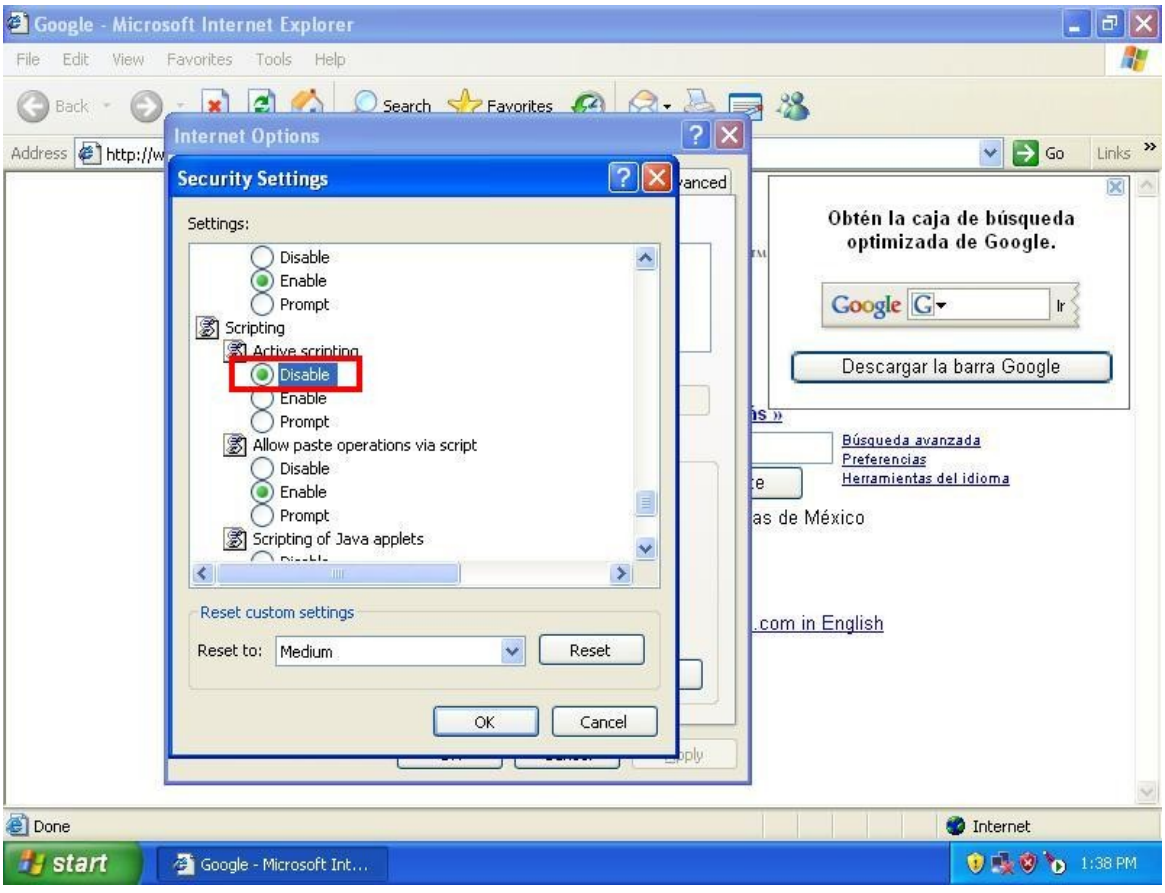
Desactivar los controles ActiveX de QuickTime en Internet Explorer

```
Windows Registry Editor Version 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
```

Desactivar Active Scripting en Internet Explorer

En la ventana de Internet Explorer, desplazarse al menú Herramientas.
Seleccionar Opciones de Internet.
Seleccionar la pestaña Seguridad.
Seleccionar nivel personalizado.
En la sección Active Scripting, seleccionar deshabilitar.
Pulsar dos veces sobre el botón Aceptar.


Google - Microsoft Internet Explorer
Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Select a Web content zone to specify its security settings.
Internet
Local intranet
Trusted sites
Restricted sites
Internet
This zone contains all Web sites you haven't placed in other zones
Sites...
Security level for this zone
Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.
Custom Level...
Default Level
OK
Cancel
Apply
Obtén la caja de búsqueda optimizada de Google.
Descargar la barra Google
Búsqueda avanzada
Preferencias
Herramientas del idioma
Done
Internet
start
Google - Microsoft Int...
1:36 PM


Google - Microsoft Internet Explorer
Internet Options
Security Settings
Settings:
Disable
Enable
Prompt
Scripting
Active scripting
Disable
Enable
Prompt
Allow paste operations via script
Disable
Enable
Prompt
Scripting of Java applets
Reset custom settings
Reset to:
Medium
Reset
OK
Cancel
Obtén la caja de búsqueda optimizada de Google.
Descargar la barra Google
Búsqueda avanzada
Preferencias
Herramientas del idioma
Done
Internet
start
Google - Microsoft Int...
1:38 PM

Referencias

[SFQT] Publicación de la vulnerabilidad en QuickTime Player
http://www.securityfocus.com/bid/26549/info

[MWQT] Prueba de concepto
http://www.milw0rm.com/exploits/4648

[CQT] Nota de vulnerabilidad US-CERT
http://www.kb.cert.org/vuls/id/659761