

## MySpace Worm + QuickTime Vuln.

Contributed by Administrator  
Friday, 08 December 2006

MySpace Worm gebruikt QuickTime Vulnerabilities (zwakheden). Uitleg van de hack

New MySpace  
worm could be on its way Dec 07 2006 03:29AM

pdp (architect) (pdp gnu citizen gmail com)

<http://www.gnucitizen.org/blog/myspace-quicktime-worm-follow-up>

MySpace was hit by a worm in a semi-automatic manner. This time the worm propagated via a QuickTime flaw found a couple of months ago.

This shouldn't be a surprise to anyone. It is quite serious that this attack vector was picked up by Apple so late.

In this post I am not going to explain how this particular MySpace hack works but rather to send a reminder to the security community that another <http://www.gnucitizen.org/blog/backdooring-mp3-files> QuickTime XSS vector was found right after the first one. This vector can be used in a similar way although, IMHO, the impact is greater. I guess Apple should fix both issues NOW: we don't want MySpace worms spreading around again, although this is very utopic to say.

Here is a brief reminder of what the XSS issue was all about.

The problems is caused by a quite useful feature called QuickTime Media Link (.qtl). The whole point of these QuickTime Media Link files is to provide means of playing media files in a more accessible way.

In this respect the developer can create a .qtl file which holds information about the media content that needs to be played plus recommended dimensions, accessibility features, control features

etc...

.qtl files can contain malicious JavaScript code that can takeover some important network device when executed for example. That's not the end of the story though. Because of its flexibility QuickTime doesn't mind if Media Link (.qtl) files end with .mp3, .mp4, .m4a or even .mov extension...

This is a quite big problem especially in default configurations of iTunes. The iTunes installation wizard installs the QuickTime player and QuickTime browser plugins and associates various media files with its components. If you open an mp3 file from the desktop it will be played in iTunes player by default, however if you open it from some website it will be played in the QuickTime player browser plugin. In this respect, users who are previewing mp3 and other media files from the Internet are vulnerable.

#### GNUCITIZEN >> Backdooring MP3 Files

To sum up, and put into context, attackers can use QuickTime Media Links to imitate popular media files and as such trick the user into opening malicious content that could lead to their (MySpace) account or their browser being compromised. Lets look at the following hypothetical situation:

"Evil Hacker decides to overtake MySpace in order to DoS google.com. He finds that MySpace allows users to supply links in their posts and comments. He spends some time to research the 1000 most popular MySpace members where he will post links to media files titled orgy.mov or myconfession.mp3 or even prankster.avi. Once an unaware user clicks on the link, a phishing page is presented asking the current user to enter their MySpace details to see the private content. If the user is tricked, their credentials will be on their

way to the specifically designed for that operation collection point where another automatic process overtakes their user account installing the same malicious file or simply hijack other media files by wrapping them up in QuickTime Media Links the same way it is described in the article mentioned above. The process repeats when another users falls into the trap. When enough number of accounts are compromised Evil Hacker will launch his/her DDoS against Google's AdSense server farm."

Before seeing more worms of this kind I suggest that we gather our intellectual power to find a fix or at least a workaround. I welcome you to join me at GNUCITIZEN's MySpace Worms Topic <<http://www.gnucitizen.org/topics/myspace-worms>> for further discussion. I can assure you that GNUCITIZEN neither me has anything to do with MySpace or any other related organization. The purpose of this symposium is learn more about these types of worms and help other online applications and communities protect themselves. This is much better than just sitting in our comfy chairs and laughing at people's mistakes.

Many thanks.

--

pdp (architect) | petko d. petkov

<http://www.gnucitizen.org>