

Forum:[Hack Forums](#)

Thread: [Movie subtitles malware\[VLC affected\]](#)

tcsh - May 23, 2017, 6:12 pm

Do you watch movies with subtitles?

Just last night, I wanted to watch a French movie, so I searched for English subtitles and downloaded it to my computer.

Though that film was excellent, this morning a new research from Checkpoint scared me.

I was unaware that a little subtitle file could hand over full control of my computer to hackers, while I was enjoying the movie.

Yes, you heard that right.

A team of researchers at Check Point has discovered vulnerabilities in four of the most popular media player applications, which can be exploited by hackers to hijack "any type of device via vulnerabilities; whether it is a PC, a smart TV, or a mobile device" with malicious codes inserted into the subtitle files.

[Full article](#)

How to Protect Your Computer?

Code Check Point has already informed the developers of VLC, Kodi, Popcorn Time and Stremio applications about the recently discovered vulnerabilities.

"To allow the developers more time to address the vulnerabilities, we've decided not to publish any further technical details at this point," the researchers said.

All of them have patched the flaws, with Stremio and VLC releasing the patched versions of their software: Stremio 4.0 and VLC 2.2.5 that has been out for two weeks.

However, Kodi developer Martijn Kaijser said the official version 17.2 release would arrive later this week, while users could get a fixed version online. A patch for Popcorn Time is also available online. So, users are advised to update their media player as soon as possible.

Cannot Compute - May 23, 2017, 6:17 pm

That's why you don't download random shit off the internet.

tcsh - May 23, 2017, 6:21 pm

(May 23, 2017 06:17 PM)Cannot Compute Wrote: [\[CITE\]](#) That's why you don't download random shit off the internet.

What does that have to do with it? It's a subtitle file, I'm sure everyone has had a problem with one of them once and used the internet. lol, your name suits you. ?

Magicmann - May 23, 2017, 6:23 pm

(May 23, 2017 06:21 PM)tcsh Wrote: [\[CITE\]](#) What does that have to do with it? It's a subtitle file, I'm sure everyone has had a problem with one of them once and used the internet. lol, your name suits you. ?

As someone that has worked in the computer industry, most infections are your own fault because you went to a sketchy site or fell for something.

Regulus - May 23, 2017, 6:24 pm

I've been using a lots of Swedish subtitles from YIFY.

I hope I am not affected.

?Ñåzg?l - May 23, 2017, 9:21 pm

(May 23, 2017 06:23 PM)Magicmann Wrote: [\[CITE\]](#) As someone that has worked in the computer industry, most infections are your own fault because you went to a sketchy site or fell for something. what he probably meant to say was that since it was not a executable file it looked harmless but the truth is malware can be hidden in anything (in a media file such as mp3 to a document file such as .doc or .pdf)

I honestly would have never expected a subtitle file to be anywhere near sketchy

to prevent this issue you need to run vlc with very low privileges and sandboxed

.BangsOnly - May 23, 2017, 11:00 pm

(May 23, 2017 09:21 PM)?Ñåzg?l Wrote: [\[CITE\]](#) what he probably meant to say was that since it was not a executable file it looked harmless

but the truth is malware can be hidden in anything (in a media file such as mp3 to a document file such as .doc or .pdf)

I honestly would have never expected a subtitle file to be anywhere near sketchy

to prevent this issue you need to run vlc with very low privileges and sandboxed

I agree. I wouldn't expect a subtitle file to be dirty but most of the time a antivirus woulda slapped me. Also most people wouldn't run vlc sandboxed. I woulda definitely gotten hit with that.

It's good to know.

COR??X - May 23, 2017, 11:42 pm

(May 23, 2017 09:21 PM)?Ñåzg?l Wrote: [\[CITE\]](#) what he probably meant to say was that since it was not a executable file it looked harmless

but the truth is malware can be hidden in anything (in a media file such as mp3 to a document file such as .doc or .pdf)

I honestly would have never expected a subtitle file to be anywhere near sketchy

to prevent this issue you need to run vlc with very low privileges and sandboxedWould like to see an exe to mp3 converter._.

Would have to be some crazy Oday shit.

tcsh - May 24, 2017, 2:07 am

(May 23, 2017 06:23 PM)Magicmann Wrote: [\[CITE\]](#) As someone that has worked in the computer industry, most infections are your own fault because you went to a sketchy site or fell for something.

Uhm, it's a subtitle file, how does downloading a subtitle file mean you "download random shit" like the dude I was referring said? :P

Anyway, just an awareness thread, be sure to update and stay safe.

gringo - May 24, 2017, 2:16 am

Very interesting, I was not aware this was a thing thanks for the heads up. I usually stream movies to my fire stick through kodi but if it's some obscure shit that I need subtitles for I'll be sure to remember this.

Reece Morgan - May 25, 2017, 1:21 am

(May 23, 2017 09:21 PM)?Ñåzg?l Wrote: [\[CITE\]](#) what he probably meant to say was that since it was not a executable file it looked harmless

but the truth is malware can be hidden in anything (in a media file such as mp3 to a document file such as .doc or .pdf)

I honestly would have never expected a subtitle file to be anywhere near sketchy

to prevent this issue you need to run vlc with very low privileges and sandboxed
It's important to note here that just because a file isn't an executable file, the code in it can still be executed. Just because something isn't .exe doesn't mean that there isn't code inside capable of being executed on your computer.

Any type of file can be used to hide malware, it's just that files are executed in different ways depending on their extension.

Silver Fang - May 25, 2017, 3:31 am

(May 25, 2017 01:21 AM)Reece Morgan Wrote: [\[CITE\]](#) It's important to note here that just because a file isn't an executable file, the code in it can still be executed. Just because something isn't .exe doesn't mean that there isn't code inside capable of being executed on your computer.

Any type of file can be used to hide malware, it's just that files are executed in different ways depending on their extension.

In this case, via a videoplayer that already have all the needed rights (?)

How does it evolve to a working executable without the player though, or is it allowed to be kept as a allowed application without the player?edit: (probably dumb question as it already had all the rights)

Nevermind.

Reece Morgan - May 25, 2017, 3:58 am

(May 25, 2017 03:31 AM)Silver Fang Wrote: [\[CITE\]](#) In this case, via a videoplayer that already have all the needed rights (?)

How does it evolve to a working executable without the player though, or is it allowed to be kept as a allowed application without the player?edit: (probably dumb question as it already had all the rights)

Nevermind.

Yes it would have been executed by the videoplayer.

Minisaints - May 25, 2017, 6:53 am

People who can't read should be okay then.

tcsh - May 25, 2017, 8:46 am

(May 25, 2017 06:53 AM)SubJectionN Wrote: [\[CITE\]](#) People who can't read should be okay then.
?? You're creative, I'll give you that!

watashiwa - May 26, 2017, 8:05 am

But isn't subtitles just a text file ? how can it infect the computer ?

tcsh - May 26, 2017, 10:32 am

(May 26, 2017 08:05 AM)watashiwa Wrote: [\[CITE\]](#) But isn't subtitles just a text file ? how can it infect the computer ?

It's code("text") at the end of the day, in the subtitle file, which the player will process. Thus you can go beyond the initial function of the subtitle and make it process specific type of code, which you then use to gain access or do other stuff. In a nutshell, If I explained it right.