

Forum:[Hack Forums](#)

Thread: [VLC is now vulnerable](#)

Elweth - June 21, 2019, 10:05 pm

Update now..

Quote:If you use VLC media player on your computer and haven't updated it recently, don't you even dare to play any untrusted, randomly downloaded video file on it.

Doing so could allow hackers to remotely take full control over your computer system.

That's because VLC media player software versions prior to 3.0.7 contain two high-risk security vulnerabilities, besides many other medium- and low-severity security flaws, that could potentially lead to arbitrary code execution attacks.

With more than 3 billion downloads, VLC is a hugely popular open-source media player software that is currently being used by hundreds of millions of users worldwide on all major platforms, including Windows, macOS, Linux, as well as Android and iOS mobile platforms.

Discovered by Symeon Paraschoudis from Pen Test Partners and identified as CVE-2019-12874, the first high-severity vulnerability is a double-free issue which resides in "zlib_decompress_extra" function of VideoLAN VLC player and gets triggered when it parses a malformed MKV file type within the Matroska demuxer.

The second high-risk flaw, identified as CVE-2019-5439 and discovered by another researcher, is a read-buffer overflow issue that resides in "ReadFrame" function and can be triggered using a malformed AVI video file.

Though the proof-of-concepts demonstrated by both researchers cause a crash, a potential attacker can exploit these vulnerabilities to achieve arbitrary code execution with the same privileges as of the target user on the system.

All the attacker needs to do is craft a malicious MKV or AVI video file and trick users into playing it using the vulnerable versions of VLC.

Well, that's not a tough job, as attackers can easily target hundreds of thousands of users within hours by simply releasing malicious video files on torrent sites, mimicking as a pirated copy of a newly released movie or TV series.

According to an advisory released by VideoLAN, having ASLR and DEP protections enabled on the system could help users mitigate the threat, but developers did admit that these protections could be bypassed too.

Paraschoudis used honggfuzz fuzzing tool to discover this issue and four other bugs, which were also patched by the VideoLAN team earlier this month along with 28 other bugs reported by other security researchers through EU-FOSSA bug bounty program.

Users are highly recommended to update their media player software to VLC 3.0.7 or later versions and should avoid opening or playing video files from untrusted third parties.

<https://thehackernews.com/2019/06/vlc-media-player-hacking.html>

debian - June 21, 2019, 10:51 pm

Wow, fucking crazy. Are there any actual reported attacks? And I'm guessing that this only affects Windows machines or what?

munf4r1dd - June 22, 2019, 7:05 am

Damn this is scary, people should be warned. Thank God I don't use it.

webdev77 - June 22, 2019, 7:09 am

Excellent reason why you should always keep software up to date.

tenten - June 22, 2019, 1:28 pm

how do I know if I was compromised?

apepi - June 22, 2019, 2:37 pm

Eh, great. Guess I'll have to be weary file sharing anytime soon.

StickTalk - June 22, 2019, 8:52 pm

(Jun 22, 2019 07:09 AM)webdev77 Wrote: [\[CITE\]](#) Excellent reason why you should always keep software up to date.

Agreed. I always check for updates daily. Especially on my work laptop.

duplex - June 26, 2019, 12:55 am

Thank you for letting us know about, highly appreciated

Takehito Morokuzu - June 26, 2019, 6:05 am

Media Player Classic Black Edition is better anyways IMO. Much more efficient on system resources and better visual quality (VLC is known to look washed out)

Cammy - June 26, 2019, 7:49 am

(Jun 26, 2019 06:05 AM)Takehito Morokuzu Wrote: [\[CITE\]](#) Media Player Classic Black Edition is better anyways IMO. Much more efficient on system resources and better visual quality (VLC is known to look washed out)

I agree, I've been using MPC + MadVR for a long time now. Shit's super OP

BennyPuP - July 11, 2019, 10:20 am

WTF just when you think Linux is Most secure and there's always away in

Pr0m3th3us - July 11, 2019, 7:09 pm

Nice find, thanks for this