Learn new vulnerabilities in VLC that allow hackers to access computers

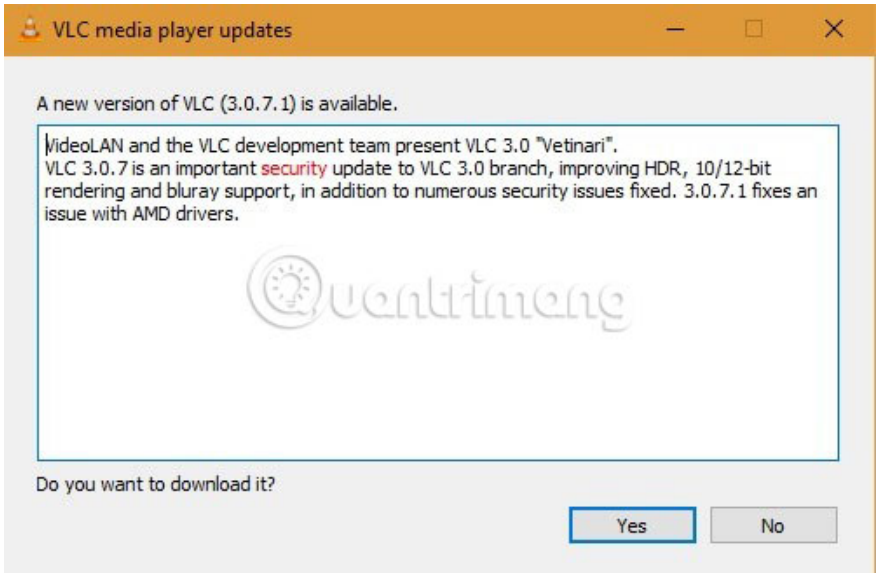
If you have VLC media player on your computer, you must immediately upgrade to the latest version, 3.0.7 or higher.

If you have VLC media player on your computer, you must immediately upgrade to the latest version, 3.0.7 or higher. There are two new exploits that allow hackers to use vulnerable versions of VLC to crash your system and execute their malicious code remotely.

Very typical attack method. After you download the attack file AVI or MKV, it will give hackers full control over the computer whenever you play video on VLC. These attack files may originate from torrent videos as well as Facebook, Twitter or Instagram.

It sounds very dangerous, right? Yes, it's because VLC's "father" of Videolan has issued a warning about this issue. In the past few days, many users have noticed the update requirements whenever they open VLC Media Player.

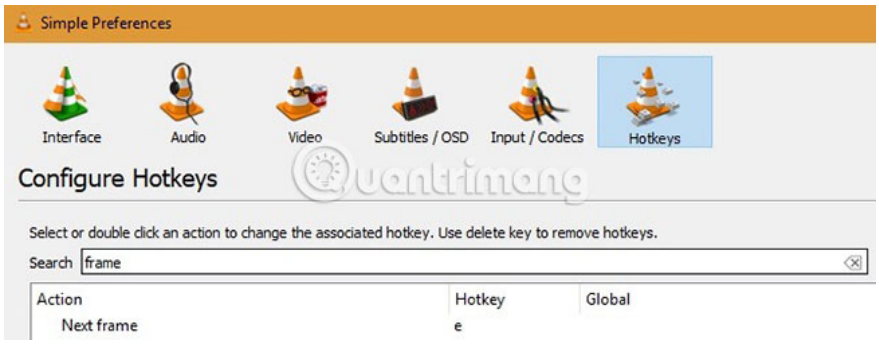
C?nh báo: Không s? d?ng giá tr? này tr??c khi b?n cài ??t phiên b?n này m?i, 3.0.7.



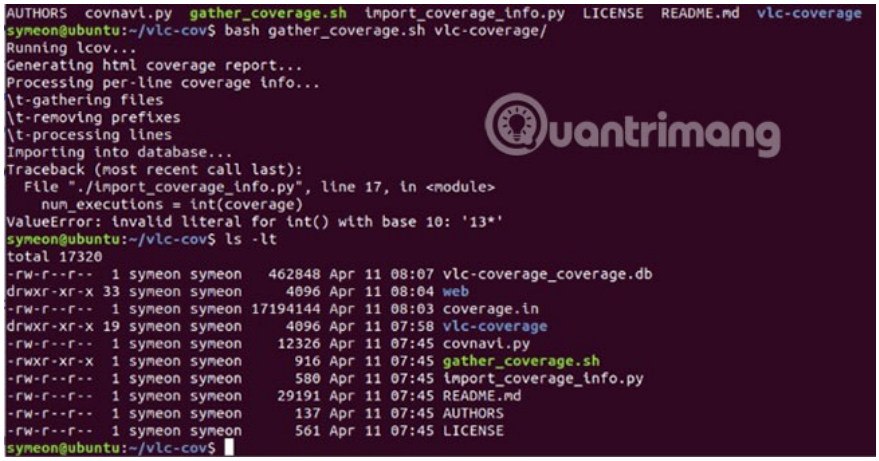
What really happened?

Occasionally this month, security researchers at Pen Test Partners developed a new exploit method aimed at older VLC versions, including 3.0.6. They call it **CVE-2019-12874,** which uses fuzzing technology to generate invalid or random data.

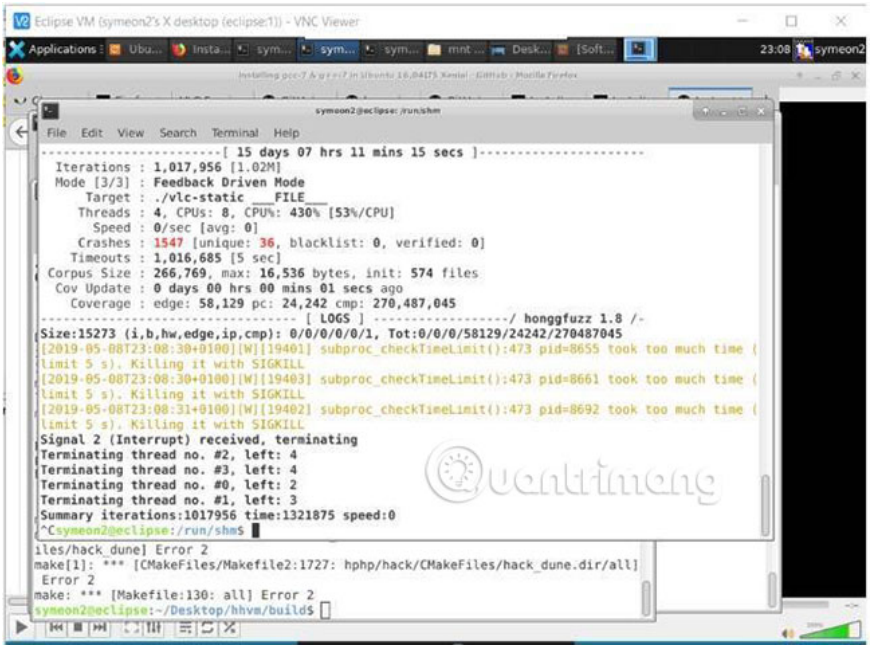
Basically, VLC is a complex software, using a large number of third-party libraries contributed by open source product developers. One of these functions, called **demux / mkv,** is in ReadFrames, which can be run in the background of VLC files in **Simple Preferences.** This feature of VLC is easily defeated by new attack vectors.



When the attack file downloads the system, you will see VLC play for 5 seconds, exit and then repeat. This problem will never end.



According to the partners of the Pen Test, so far they have implemented 1 million times this exploit method and had 1547 successful cases. So far, many of the hundreds of millions of VLC users don't know about this threat.



In addition to the remote incident exploitation above, another buffer overflow vulnerability, named CVE-2019-5439, was also revealed on June 12, 2019. This vulnerability also uses the ReadFrame function of VLC to prompt users to download specially created AVI or MKV files. If a successful buffer overflow is caused, hackers can cause the system to crash or remotely exploit.

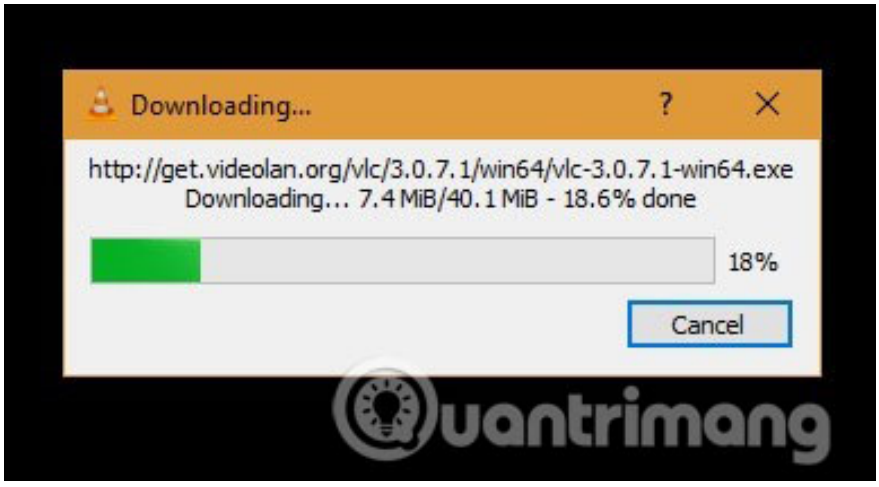
How does the latest VLC Media Player version solve these problems?

According to the latest release of VLC, version 3.0.7 fixes the problem by fixing buffer overflow errors for some file extensions, including MP4, MKV, AVI and NSC. It also prevents infinite loops from running when an invalid item is playing.

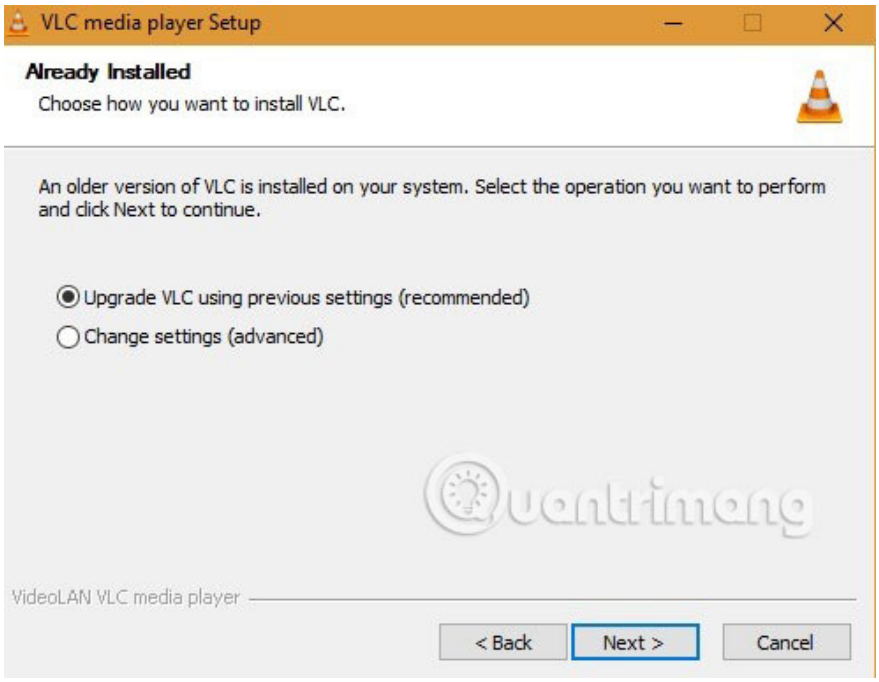
https://www.videolan.org/developers/vlc-branch/NEWS

```
Changes between 3.0.7 and 3.0.7.1:
----------------------------------

Access:
 * Update libbluray to 1.1.2

macOS:
 * Fix bluray java menu playback regression in 3.0.7

Video Output:
 * Fix hardware acceleration with some AMD drivers
 * Improve direct3d11 HDR support

Changes between 3.0.6 and 3.0.7:
--------------------------------

Security:
 * Fix multiple buffer overflows in the ps demuxer
 * Fix a buffer overflow when copying a biplanar YUV image
 * Fix multiple buffer overflows in the faad decoder
 * Fix buffer overflow in the svcdsub decoder
 * Fix buffer overflows in the ogg muxer & demuxer
 * Fix buffer overflows in libavformat demuxer
 * Fix multiple buffer overflows in the MKV demuxer
 * Fix a buffer overflow in the MP4 demuxer
 * Fix a buffer overflow in the textst decoder
 * Fix a buffer overflow in the webvtt decoder
 * Fix a buffer overflow in the ASF demux
 * Fix a buffer overflow in the UPNP SD
 * Fix use after free in the ogg demuxer
 * Fix multiple use after free in the MKV demuxer
 * Fix multiple use after free in the DMO decoder
 * Fix integer underflow in the MKV demuxer
 * Fix an updater NULL pointer dereference on invalid signing keys
 * Fix NULL pointer dereference in the MKV demuxer
 * Fix an integer overflow in the spudec decoder
 * Fix an integer overflow in the nsc demuxer
 * Fix an integer overflow in the avi demuxer
 * Fix reads of uninitialized pointers in the MKV demuxer
 * Fix a floating point exception in the MKV demuxer
 * Fix an infinite loop in the flac packetizer
```

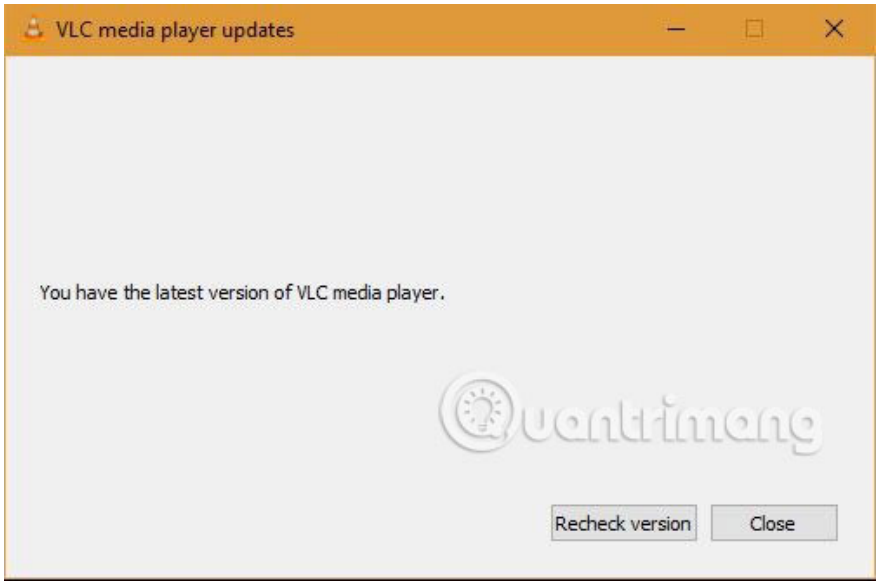
Although the patch is available, both **CVE-2019-5439** and **CVE-2019-12874** are still pending analysis by security researchers. However, at least you should download the latest VLC version from Help **/ Check for Updates** . The download will take place automatically.



Once completed, you should upgrade VLC from previous settings.



Please make sure that you download the latest version from time to time, as new errors may occur in the future and you don't know anything about it. Also, do not open any unreliable files on VLC in the present or future.



Alternatives to VLC Media Player

If you feel that VLC Media Player is not worth the risk, you may want to consider alternatives, including KM Player, Microsoft Photos, DivX and Windows Media Player. All of these options were created to run the latest h.265 codec and are great for HD video, as well as Full HD.

Have you noticed this latest vulnerability in VLC Media Player or is it the first time you've heard of it? What is your favorite media player? Share ideas with people in the comment section below, if you have problems with VLC or other media players in the past.

You finished reading the article "**Learn new vulnerabilities in VLC that allow hackers to access computers**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
