Jean Baptiste-Kempf

I'm excited to announce the release of VLC 1.0!
1,000,000 downloads per day

450,000,000 users on all platforms! *

3,200,000,000 + downloads since the early days
Dependencies
Security

• Lots of code
  - 15 millions of LoC in C, C++, ASM (handcrafted)
  - 100+ dependencies
  - Code from the early 2000s
  - Quality is...
  - Many users

• Multiple answers
  - Reviewing
  - Analysis
  - Hardening
  - Signing
  - Bug bounties
Security answers

- **Reviews**
  - Difficult and long
  - Dependency selection

- **Analysis**
  - Daily static analysis
    - Coverity, LGTM, ...
    - Cppcheck, clang
  - Dynamic analysis
    - Most developers do now
  - Fuzzing
    - Oss-fuzz and our own
  - CI/CD
• Hardening (3.0.x)
  - Fewer warnings, more compilers
  - ASLR, HEASLR (64bits)
  - DEP/NX, SEH
  - SSP
    • Stack-Protection Strong
  - WinRT/UWP
  - PIE/PIC
    • Android
Answers, part 3

- Compiling & Signing
  - Compiling on clean virtual machines, destroyed after use
  - Compiling the toolchain from source, all dependencies, tools and then VLC
  - Taken by the maintainer, tested
  - Code Signing with HSM (yubikeys), and GPG-signed (maintainer)
  - Uploaded to development server
  - Downloaded and checked by FTP-master
  - Signed with VideoLAN GPG keys
    - HSM (Yubikeys), offline
  - Pushed on the release server
Bug Bounties

• EU-FOSSAv2 program
  - V1 was security analysis

• Personnaly Dislike
  - Money for finding bugs, not fixing them
  - Money for open source is a hot topic those days

• However
  - Prices for exploits on VLC are a bit high already
  - Want to help the EU to do more about open source
  - Try and see what happens
  - Extra bounties for patches provided
FOSSA results

- 31 security issues found in 3.0
  - 1 high
    - OOB write
    - *not in VLC*
  - 20 medium
    - OOB read, crash, Null deref, double-free
  - 10 low
    - Integer underflows, some OOB, parsing issues, busy-loops

- HackerOne team
  - OK-ish in communication
  - Price is high
FOSSA results 2

• Hackers
  - From the best to the worst
    • requesting answers and reproducibility in < 24h, and sending 10 mails in the mean time;
    • sending the same issue more than 10 times, because the stacktracs are slightly different; and complain only one bounty awarded;
    • refusing to read the guidelines, and refusing to test the good version, and then insulting us;
    • aggressivity, or insults, to the point where the HackerOne team had to intervene several times;
    • plugging the output of their fuzzer to HackerOne without checking if it actually crashes or if it is a different bug;
    • submitting the same bug to a different program (Google Android Apps) to get 2 times the bounty, while the bug DID NOT apply on Android, but without checking;
    • ...

PassTheSalt
Personal opinion: yes, you are overall very bad. We have only negative feedback from interacting with this community. It is always insults, death threats and clueless people. And never people who try to talk and discuss.
Half of the reports we have are total crap:
- “I found the source code of VLC”
- “I found the source code of your website”
- “I found an open folder on your FTP/HTTP”
- “Your jenkins|gitlab|trac is open”
- “Those ports are open on your servers”

So many reports are not signed, not to the right contact or just on our public tracker...
• Overblowing everything
  – A security issue is a bug.
    • We will fix it. But calm down
      It does not mean I will stop my life right now for it.
      It was a bug yesterday; most people will not update tomorrow.
  – Stop abusing CVSS
    • If all your security issues are > 9, the scale means nothing
    • Because your WinDbg scripts stays Exploitable does not mean it is
    • Every file can be on the internet with a playlist
      – This is not a remote execution…
    • We cannot get CVE…

• Extreme Clickbaiting
Code Execution Flaw (CVE-2018-4013) Discovered in LIVE555 Media Streaming Library Leaves #VLC, Other Media Players and CCTV Streaming Applications Vulnerable to #Hacking

thehackernews.com/2018/10/critic …

#infosec #cybersecurity

Beware! Playing Untrusted Videos On VLC Player Could Hack Your Computer

June 21, 2019 · Swati Khandewal

If you use VLC media player on your computer and havent updated it recently, dont 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.

Thats 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 Symoons Paraschosoudis 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-2016-4316 and discovered by another researcher in a near-
• Mauvaise Foi
  - HTTP updates
• Always the same
  - “OMG, updates are over HTTP”
  - “OMG, VLC is insecure and trivial to replace the update”
  - Write articles or Twitter posts
  - “Well, no, the updates are GPG signed, so it does not matter how the updates are served”
  - “Oh, but what about...”
• Downgrade attacks
  - Managed in the installer

• Stay the same version
  - Same as blackholing update.videolan.org

• You should not use your own crypto
  - DSA/RSA are not "our own"
    - Gcrypt, GnuTLS

• VideoLAN website does not have the **right TLS**
  - Whatever TLS option some people want and fight about

• You update your .asc over HTTP
  - Yes, but it is signed

• You use sha1…

• But privacy!
  - You contact update.videolan.org, man…
VLC developers refused to consider "update-over-HTTP" as a threat.

Responded—a "no threat model, no proof, no security bug"

It wouldn't hurt if you simply consider the suggestion.

trac.videolan.org/vlc/ticket/217...
• And then we have the Italian InfoSec community
  - HTTPS update
  - Refused to discuss privately
  - Insults
  - Created github pages to doxx VLC developers
  - DDOS from Italy in the next days after
  - Go on every Social Media post to spit on VLC
    - “French Government”
  - No solution whatsoever
• **VLC.js**
  - Html5 video suxx
  - Flash Server + Player was nice
  - VLC inside a browser with WebAsm
  - Ads, more format support, fast, evolutive

• **Hardening VLC**
  - VLC security is hard
  - No hardened player
  - Better streaming solutions
  - Important cost