

Inside the media.

Security vulnerabilities in multimedia processing.

A case study of FFmpeg

Abdelaziz Hazem Abdullallah

6681

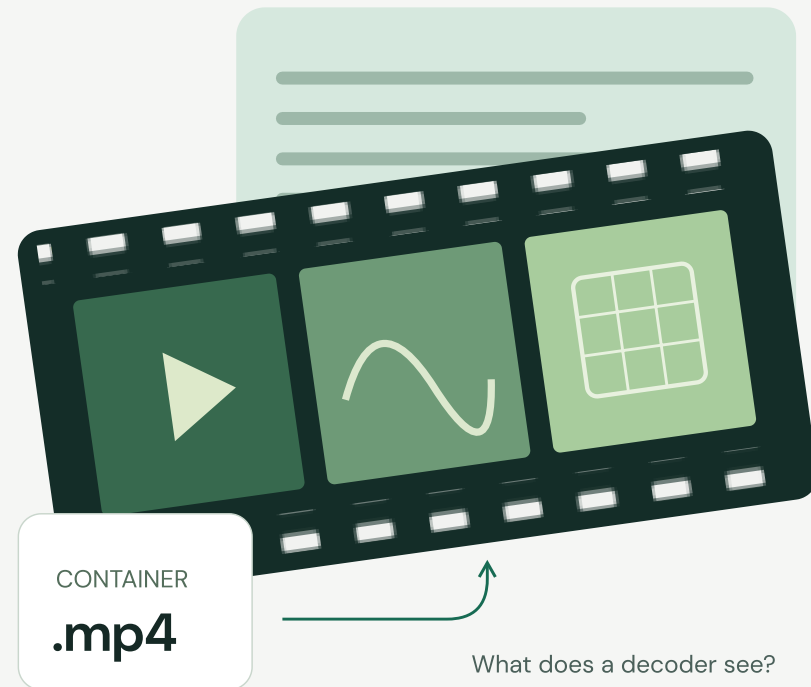
Hamza Ahmed Faraj Ruhaet

6350

Fares Mohammed Hamad El-Malki

6325

Academic research presentation · Names and student IDs



— More structure. More assumptions.

A video is more than pixels.

The container

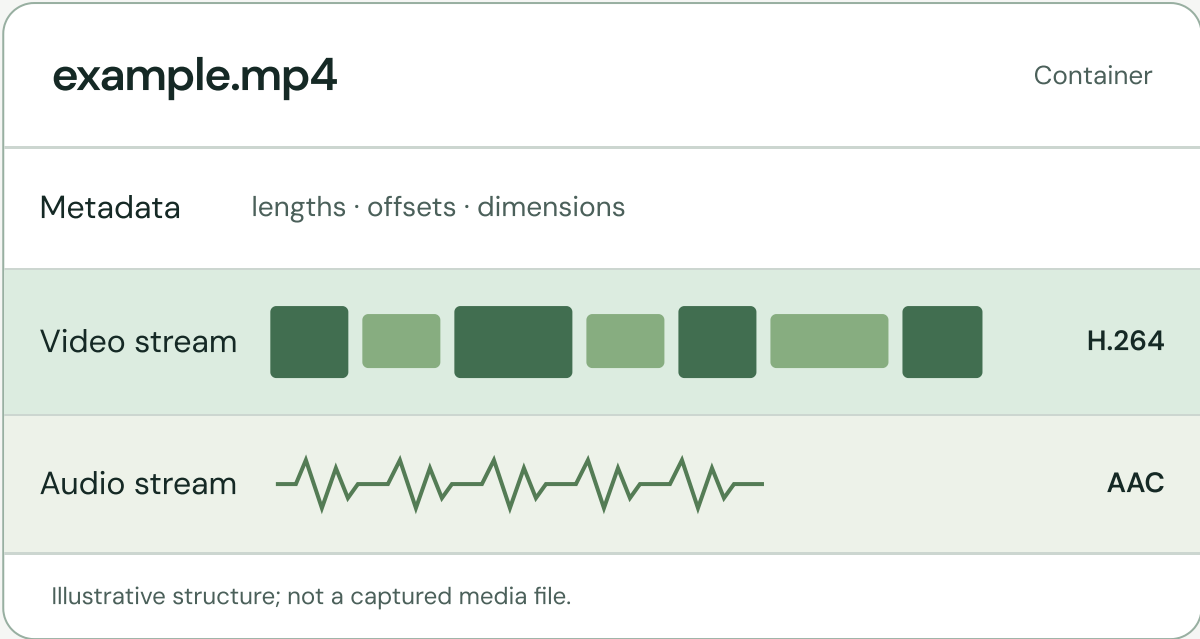
MP4 organizes streams, timestamps, and metadata.

The codec

H.264 defines how compressed video becomes frames.

 The extension does not tell you whether every internal relationship is valid.

What looks like one file is a set of relationships the software has to trust—or check.



Untrusted file → Application → Parser / decoder

A reachable defect creates risk.

One tool. Many boundaries.

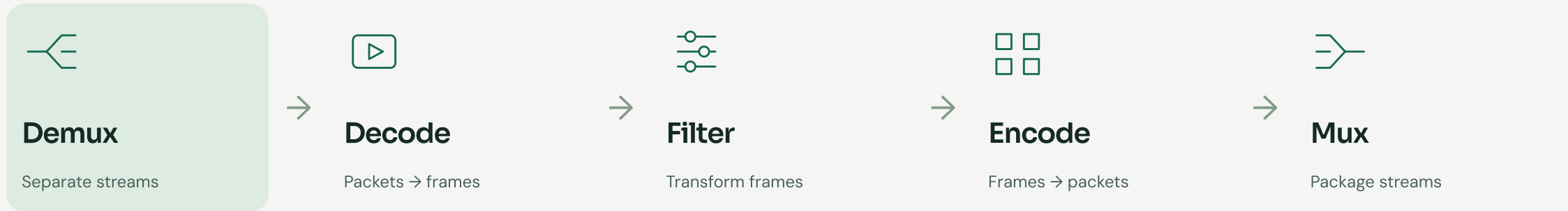
ffmpeg coordinates the work. Its libraries can also run inside other applications.

Transcoding

Stream copy

Input media

Output media



libavformat

The demuxer reads a container and separates its encoded streams into packets.

A typical transcoding path. Filters are optional; real pipelines can contain several streams.

A small assumption. A large consequence.

Malformed input matters when an implementation mishandles a bound, a dimension, or an object's lifetime.

Allocated buffer



A missing bounds check can cross this line.

Conceptual diagram, not an exploit demonstration.

Read

Write

Lifetime

Out-of-bounds read

Access beyond an intended region can crash a process or expose information.

A crash is a finding.

Code execution requires additional evidence.

Structure gets past the first gate.

Template

Describe a binary format



Structured inputs

Generate + mutate; integrate with AFL



FFmpeg

Direct MP4 and AVI processing tests

FormatFuzzer turns binary-format templates into parsers, generators, and mutators. [\[1\]](#)

Reported in the tested FFmpeg configuration

Segmentation faults. Aborts. Investigation.

Threading enabled 200 MB memory limit

Crash observations establish failures—not a proven exploit for every input.

Detailed findings checked in the corresponding author manuscript. Final journal metadata and abstract verified.

When decoding changes state.

H.264

Sequence parameters change

Reinitialize
hardware context



A stale reference remains

Use-after-free

H26Forge edits H.264 syntax elements while preserving syntactic structure—even with semantically non-compliant values. [2]

The precise FFmpeg connection

libavcodec in VLC 3.0.17 on Windows, through the Direct3D11 hardware path.

Historical, configuration-specific findings. The VLC discussion describes possible code execution, not a complete demonstrated exploit.

The broader study

Other findings concerned Firefox and tested iOS / Android decoder stacks. They retain their own attribution.

Give a failure less room.

Test continuously.

Format-aware fuzzing, malformed inputs, and regression cases.

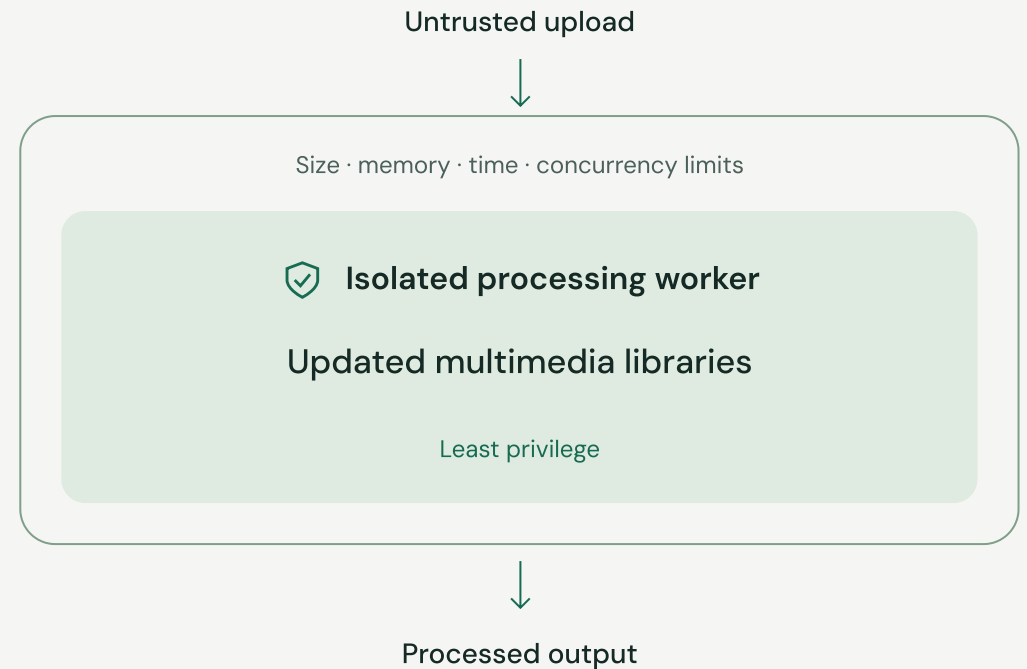
Build defensively.

Check bounds and lifetimes. Use memory-safe components where feasible.

Keep it maintained.

Update dependencies and retest the deployed configuration.

Reduce the chance of a defect.
Reduce the reach of a compromised worker.



Isolation has limits: a userspace sandbox does not automatically contain privileged hardware-driver flaws.

Treat media as structured, untrusted input.

Understand the path. Test the assumptions.
Contain the consequences.

The research behind the story

- [1] R. Dutra, R. Gopinath, and A. Zeller, “FormatFuzzer: Effective Fuzzing of Binary File Formats,” ACM Transactions on Software Engineering and Methodology, vol. 33, no. 2, Art. no. 53, pp. 53:1–53:29, 2024, doi: 10.1145/3628157.
- [2] W. R. Vasquez, S. Checkoway, and H. Shacham, “The Most Dangerous Codec in the World: Finding and Exploiting Vulnerabilities in H.264 Decoders,” in Proceedings of the 32nd USENIX Security Symposium, Anaheim, CA, USA, Aug. 2023, pp. 6647–6664. USENIX Association.
- [3] FFmpeg Project, “ffmpeg Documentation,” §§3–3.1. Accessed: Oct. 26, 2026. [Online]. Available: <https://ffmpeg.org/ffmpeg.html>.

[1] Detailed findings verified in the corresponding author manuscript; final publisher full text was inaccessible. [3] verifies functionality, not experimental security results.