#8186 closed defect (fixed)

double-free/heap-use-after-free when remuxing rtp hint tracks

Reported by:	Suhwan	Owned by:	
Priority:	important	Component:	avformat
Version:	git-master	Keywords:	asan
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	no
Analyzed by developer:	no		

Description

Summary of the bug:
There is a heap-use-after-free from libavutil/mem.c:231:5 in av_freep

```
SUMMARY: AddressSanitizer: heap-use-after-free ffmpeg/libavutil/mem.c:231:5 in a
```

How to reproduce:

```
% ./ffmpeg_g -t 0 -stream_loop 25 -y -i chris.mov -loglevel 0 -map 0 -c copy -c:v:

ffmpeg version N-94982-gea673a0edb Copyright (c) 2000-2019 the FFmpeg developers
  built with clang version 6.0.0-1ubuntu2 (tags/RELEASE_600/final)
  configuration: --cc=clang --cxx=clang++ --ld=clang --enable-debug --toolchain=cl
```

◀   ▶

Attachments (2)

- ASAN-UAF-av_freep(3.1 KB) - added by Suhwan 3 years ago.
- chris.mov(744.1 KB) - added by Suhwan 3 years ago.
  poc

Change History (3)

---

by Suhwan, 3 years ago

    Attachment: *ASAN-UAF-av_freep*added

by Suhwan, 3 years ago

    Attachment: *chris.mov*added

    poc

comment:1 by mkver, 2 years ago

    Component: undetermined → avformat
    Resolution: → fixed
    Status: new → closed
    Summary: heap-use-after-free from libavutil/mem.c:231:5 in av_freep → double-free/heap-use-after-free when remuxing rtp hint tracks

    Fixed in 22c3cd176079dd104ec7610ead697235b04396f1.

Note: See TracTickets for help on using tickets.