#8188 closed defect (fixed)

Opened 3 years ago
Closed 22 months ago
Last modified 22 months ago

heap-use-after-free from libavformat/mpegenc.c in mpeg_mux_write_packet

Reported by:	Suhwan	Owned by:	
Priority:	important	Component:	avformat
Version:	git-master	Keywords:	mpegps 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 libavformat/mpegenc.c in mpeg_mux_write_packet.

```
SUMMARY: AddressSanitizer: heap-use-after-free ffmpeg/libavformat/mpegenc.c:1187:3
```

How to reproduce:

```
% ./ffmpeg_g -stream_loop 14 -y -r 115 -i Event20120111133101017.avi -loglevel 0 -

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)

- Event20120111133101017.avi(544.9 KB) - added by Suhwan 3 years ago.
  poc
- ASAN-UAF-mpeg_mux(3.1 KB) - added by Suhwan 3 years ago.

Change History (4)

by Suhwan, 3 years ago

Attachment: *Event20120111133101017.avi*added

poc

by Suhwan, 3 years ago

Attachment: *ASAN-UAF-mpeg_mux*added

comment:1 by mkver, 22 months ago

Component: undetermined → avformat
Resolution: → fixed
Status: new → closed

Fixed in cfce16449cb815132f829d5a07beb138dfb2cba6.

comment:2 by Carl Eugen Hoyos, 22 months ago

Keywords: mpegps added

Note: See TracTickets for help on using tickets.