Opened 3 years ago
Closed 3 years ago
Last modified 3 years ago

#8183 closed defect (fixed)

heap-buffer-overflow at libavcodec/get_bits.h writing mov files

Reported by:	Suhwan	Owned by:	
Priority:	important	Component:	avformat
Version:	git-master	Keywords:	asan mov
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	yes
Analyzed by developer:	yes		

Description

Summary of the bug:
There is a heap-buffer-overflow bug at libavcodec/get_bits.h:403:5

```
SUMMARY: AddressSanitizer: heap-buffer-overflow ffmpeg/./libavcodec/get_bits.h:403
```

How to reproduce:

```
% ./ffmpeg_g -t 3 -y -r 82 -i test_v_av1_320x180.webm -loglevel 99 -map 0 -c copy

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-get_bits(3.3 KB) - added by Suhwan 3 years ago.
- test_v_av1_320x180.webm(27.5 KB) - added by Suhwan 3 years ago.
  poc

Change History (4)

by Suhwan, 3 years ago

Attachment: *asan-get_bits*added

by Suhwan, 3 years ago

Attachment: *test_v_av1_320x180.webm*added

poc

comment:1 by James, 3 years ago

Analyzed by developer:	set
Component:	undetermined → avformat
Reproduced by developer:	set
Resolution:	→ fixed
Status:	new → closed

Fixed in 58aa0ed8f10753ee90f4a4a1f4f3da803cf7c145

comment:2 by Carl Eugen Hoyos, 3 years ago

Keywords:	mov added
Summary:	heap-buffer-overflow at libavcodec/get_bits.h → heap-buffer-overflow at libavcodec/get_bits.h writing mov files

Note: See TracTickets for help on using tickets.