#8263 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

signed integer overflow at libavfilter/vf_convolution.c:139

Reported by:	Suhwan	Owned by:	
Priority:	normal	Component:	undetermined
Version:	git-master	Keywords:	ubsan
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	no
Analyzed by developer:	no		

Description

Summary of the bug:
There are 3 signed integer overflow and 1 outside the range of representable values of type 'int' at libavfilter/vf_convolution.c:139

I compiled ffmpeg with "--toolchain=clang-usan" to check the undefined-behaviours and attached log file.
How to reproduce:

```
% ffmpeg_g -y -i $PoC -filter_complex roberts -target dvd -loglevel 0 tmp.subviewe

ffmpeg version N-95336-g4f4334bcbc Copyright (c) 2000-2019 the FFmpeg developers
built with clang version 6.0.0-lubuntu2 (tags/RELEASE_600/final)
configuration: --cc=clang --cxx=clang++ --ld=clang --enable-debug --toolchain=clan
```

Here's UBSAN log

```
libavfilter/vf_convolution.c:139:48: runtime error: signed integer overflow: -6553
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior libavfilter/vf_convolution
libavfilter/vf_convolution.c:139:36: runtime error: signed integer overflow: 65535
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior libavfilter/vf_convolution
libavfilter/vf_convolution.c:139:26: runtime error: -nan is outside the range of r
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior libavfilter/vf_convolution
libavfilter/vf_convolution.c:139:42: runtime error: signed integer overflow: 17120
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior libavfilter/vf_convolution
```

Please confirm.
Thanks

Attachments (2)

- gdb-vf_convolution_139(18.7 KB) - added by Suhwan 3 years ago.
- PoC_vf_convolution_139.png48(12.4 KB) - added by Suhwan 3 years ago.
  poc

Change History (3)

by Suhwan, 3 years ago

Attachment: *gdb-vf_convolution_139*added

by Suhwan, 3 years ago

Attachment: *PoC_vf_convolution_139.png48*added

poc

comment:1 by Elon Musk, 3 years ago

Resolution: → fixed
Status: new → closed

Note: See TracTickets for help on using tickets.