#7989 closed defect (fixed)

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

heap-buffer-overflow at apng_do_inverse_blend in libavcodec/pngenc.c

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

Description

Summary of the bug:
There's a heap-buffer-overflow at apng_do_inverse_blend in libavcodec/pngenc.c
q

How to reproduce:

```
% ffmpeg_g -y -r 73 -i tmp.pbm -map 0 -c:v apng -c:a pcm_dvd -disposition:a ac3_fi

ffmpeg version : N-94163-g664a27ea40

built with clang version 9.0.0 (https://github.com/llvm/llvm-project.git 442a12056
```

Patches should be submitted to the ffmpeg-devel mailing list and not this bug tracker.

Attachments (2)

- gdb_log_7989(7.2 KB) - added by Suhwan 3 years ago.
- tmp.pbm(21.9 KB) - added by Suhwan 3 years ago.

Change History (7)

by Suhwan, 3 years ago

Attachment: *gdb_log_7989*added

by Suhwan, 3 years ago

Attachment: *tmp.pbm*added

comment:1 by Suhwan, 3 years ago

code : libavcodec/pngenc.c,
I think it might happen on following line.
`if (!memcmp(input_data + bpp * x, output_data + bpp * x, bpp))`
bpp's size is bigger than the size of output_data + bpp * x.

```
static int apng_do_inverse_blend(AVFrame *output, const AVFrame *input,
                                 APNGFctlChunk *fctl_chunk, uint8_t bpp)
{
    // output: background, input: foreground
    // output the image such that when blended with the background, will produce the

    unsigned int x, y;
    unsigned int leftmost_x = input->width;
    unsigned int rightmost_x = 0;
    unsigned int topmost_y = input->height;
    unsigned int bottommost_y = 0;
    const uint8_t *input_data = input->data[0];
    uint8_t *output_data = output->data[0];
    ptrdiff_t input_linesize = input->linesize[0];
    ptrdiff_t output_linesize = output->linesize[0];

    // Find bounding box of changes
    for (y = 0; y < input->height; ++y) {
        for (x = 0; x < input->width; ++x) {
            if (!memcmp(input_data + bpp * x, output_data + bpp * x, bpp))
                continue;

            if (x < leftmost_x)
                leftmost_x = x;
            if (x >= rightmost_x)
                rightmost_x = x + 1;
            if (y < topmost_y)
                topmost_y = y;
            if (y >= bottommost_y)
                bottommost_y = y + 1;
        }

        input_data += input_linesize;
        output_data += output_linesize;
    }
```

comment:2 by Suhwan, 3 years ago

Received SIGABRT due to free invalid pointer at FFmpeg4.12

```
ffmpeg version N-94906-gcb8d6a4e3e 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=cla
  libavutil      56. 35.100 / 56. 35.100
  libavcodec     58. 56.101 / 58. 56.101
  libavformat    58. 32.104 / 58. 32.104
  libavdevice    58.  9.100 / 58.  9.100
  libavfilter     7. 58.102 /  7. 58.102
  libswscale      5.  6.100 /  5.  6.100
  libswresample   3.  6.100 /  3.  6.100
Input #0, pbm_pipe, from 'tmp.pbm':
  Duration: N/A, bitrate: N/A
    Stream #0:0: Video: pbm, monow, 560x320, 25 tbr, 25 tbn, 25 tbc
Stream mapping:
  Stream #0:0 -> #0:0 (pbm (native) -> apng (native))
Press [q] to stop, [?] for help
[swscaler @ 0xa2327c0] full chroma interpolation for destination format 'monob' not
Output #0, image2, to 'tmp_.pgm':
  Metadata:
```

```
    encoder         : Lavf58.32.104
    Stream #0:0: Video: apng, monob, 560x320, q=2-31, 200 kb/s, 73 fps, 73 tbn, 73 t
    Metadata:
      encoder         : Lavc58.56.101 apng
free(): invalid pointer
Aborted
```

comment:3 by Elon Musk, 22 months ago

Resolution: → fixed
Status: new → closed

Fixed in 5d9f44da460f781a1604d537d0555b78e29438ba

comment:4 by Carl Eugen Hoyos, 22 months ago

Component: undetermined → avcodec
Keywords: apng crash added; enc removed
Version: unspecified → git-master

comment:5 by Balling, 22 months ago

Yeah, that is what was forgotten in 372aa0777aaacf726de7cd7dd0e6797026a124ee, right? Is it possible in theory to add that to apng though?

Note: See TracTickets for help on using tickets.