

#8673 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

UAF while parsing m3u8 files (in av_probe_input_format3)

Reported by:	Assaf Sion	Owned by:	Steven Liu
Priority:	important	Component:	avformat
Version:	git-master	Keywords:	
Cc:	assafsion@gmail.com, liug05@kuaishou.com, assafsion@gmail.com	Blocked By:	
Blocking:		Reproduced by developer:	no
Analyzed by developer:	no		

Description

While trying to parse a crafted m3u8 playlist file:
ffmpeg -i input_file

ffmpeg version N-97763-g353aecbb28 Copyright (c) 2000-2020 the FFmpeg developers

```
built with clang version 6.0.0-1ubuntu2 (tags/RELEASE_600/final)
configuration: --cc=clang --extra-cflags='-O2 -g3 -fsanitize=address -fno-omit-frame-pointer
-Wno-error' --extra-ldflags='-O2 -g3 -fsanitize=address -fno-omit-frame-pointer -Wno-error'
--enable-debug --prefix=/home/cyber/VulnResearch/ffmpeg/clean/out_2
libavutil 56. 45.100 / 56. 45.100
libavcodec 58. 84.100 / 58. 84.100
libavformat 58. 43.100 / 58. 43.100
libavdevice 58. 9.103 / 58. 9.103
libavfilter 7. 80.100 / 7. 80.100
libswscale 5. 6.101 / 5. 6.101
libswresample 3. 6.100 / 3. 6.100
```

Splitting the commandline.
Reading option '-v' ... matched as option 'v' (set logging level) with argument '9'.
Reading option '-loglevel' ... matched as option 'loglevel' (set logging level) with argument '99'.
Reading option '-i' ... matched as input url with argument './bug.m3u8'.
Reading option 'out.avi' ... matched as output url.
Finished splitting the commandline.
Parsing a group of options: global .
Applying option v (set logging level) with argument 9.
Successfully parsed a group of options.
Parsing a group of options: input url ./bug.m3u8.
Successfully parsed a group of options.
Opening an input file: ./bug.m3u8.
[NULL @ 0x61b000000080] Opening './bug.m3u8' for reading
[file @ 0x610000000040] Setting default whitelist 'file,crypto,data'
Probing hls score:100 size:112
[hls @ 0x61b000000080] Format hls probed with size=2048 and score=100
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[hls @ 0x61b000000080] new_program: id=0x0000
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000000200] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] HLS request for url './au_to0.ts', offset 0, playlist 0
[hls @ 0x61b000000080] Opening './au_to0.ts' for reading
[hls @ 0x61b000000080] Failed to open segment 0 of playlist 0
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x6130000003c0] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000000580] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000000740] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000000900] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000000ac0] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000000c80] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000000e40] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000001000] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x6130000011c0] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000001380] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000001540] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x613000001700] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x6130000018c0] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
(snippet)
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION❖❖ #EXT-X-MEDIA-SEQUENCE:0')
[AVIOContext @ 0x61300001f300] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading

```

[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION:0')
[AVIOContext @ 0x61300001f4c0] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION:0')
[AVIOContext @ 0x61300001f680] Statistics: 112 bytes read, 0 seeks
[hls @ 0x61b000000080] Opening './bug.m3u8' for reading
[hls @ 0x61b000000080] Skip ('#EXT-X-VERSION:3')
[hls @ 0x61b000000080] Skip ('#EXT-X-TARGETDURATION:0')
[AVIOContext @ 0x61300001f840] Statistics: 112 bytes read, 0 seeks
=====
==123139==ERROR: AddressSanitizer: heap-use-after-free on address 0x602000000510 at pc
0x00000047dba8 bp 0x7fff6d502d10 sp 0x7fff6d5024c0
READ of size 2 at 0x602000000510 thread T0

#0 0x47dba7
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x47dba7)
#1 0xcb7da4
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0xcb7da4)
#2 0xcb87e8
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0xcb87e8)
#3 0xcb8a75
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0xcb8a75)
#4 0xcd4655
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0xcd4655)
#5 0xf7a27b
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0xf7a27b)
#6 0x51a007
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x51a007)
#7 0x518e06
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x518e06)
#8 0x518855
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x518855)
#9 0x55799f in main
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x55799f)
#10 0x7f02af8c6b96 in libc_start_main/build/glibc-OTS/EL5/glibc-2.27/csu/./csu/libc-
start.c:310
#11 0x420009 in init
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x420009)

0x602000000510 is located 0 bytes inside of 12-byte region [0x602000000510,0x60200000051c)
freed by thread T0 here:

#0 0x4dfcf0 in interceptor_free
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x4dfcf0)
#1 0xcdb258
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0xcdb258)
#2 0xcdb4c
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0xcdb4c)
#3 0xc41d25
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0xc41d25)

previously allocated by thread T0 here:

#0 0x4e0340 in interceptor_realloc
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x4e0340)
#1 0x394dee8
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x394dee8)
#2 0xcd34b2
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0xcd34b2)
#3 0xf7a27b
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0xf7a27b)
#4 0x51a007
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x51a007)
#5 0x518e06
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x518e06)
#6 0x518855
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x518855)
#7 0x55799f in main
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x55799f)
#8 0x7f02af8c6b96 in libc_start_main/build/glibc-OTS/EL5/glibc-2.27/csu/./csu/libc-
start.c:310

SUMMARY: AddressSanitizer: heap-use-after-free
(/home/cyber/VulnResearch/ffmpeg/clean/13_5_ffmpeg/FFmpeg/ffmpeg+0x47dba7)
Shadow bytes around the buggy address:
0x0c047fff8050: fa fa fd fd fa fa fd fa fa fa fd fd fa fa fd fd
0x0c047fff8060: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fa
0x0c047fff8070: fa fa fd fd fa fa 00 06 fa fa 02 fa fa fa 00 00
0x0c047fff8080: fa fa 02 fa fa fa 00 03 fa fa fd fd fa fa 00 01
0x0c047fff8090: fa fa 03 fa fa fa 00 fa fa fa 00 fa fa 00 fa

=>0x0c047fff80a0: fa fa[fd]fd fa fa fd fa fa fa 00 fa fa 00 00

0x0c047fff80b0: fa fa 02 fa fa fa 00 00 fa fa 03 fa fa fa fd fd
0x0c047fff80c0: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fa
0x0c047fff80d0: fa fa fd fa fa fa fd fd fa fa fd fa fa fa fd fd
0x0c047fff80e0: fa fa fd fa fa fa fd fa fa fa fd fd fa fa fd fa
0x0c047fff80f0: fa fa fd fd fa fa fd fd fa fa fd fa fa fa fd fa

Shadow byte legend (one shadow byte represents 8 application bytes):

Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
Left alloca redzone: ca
Right alloca redzone: cb

==123139==ABORTING

This inside av_probe_input_format3 while accessing the pointer lpd.filename at line 168 (format.c).
During the call to parse_playlist you free this pointer (hls.c:949, a call to free_segment_dynarray).

```

Attachments (1)

- **input(112 bytes)** - added by Assaf Sion 3 years ago.
PoC to trigger the bug

PoC to trigger the bug

Owner: set to Assaf Sion

comment:2 by Steven Liu, 3 years ago

maybe I need some conditions to reproduce the bug?

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

comment:3 by Assaf Sion, 3 years ago

Make sure to compile with `fsanitize=address`.

My configuration:

```
--cc=clang --extra-flags='-O2 -g3 -fsanitize=address -fno-omit-frame-pointer -Wno-error' --extra-ldflags='-O2 -g3 -fsanitize=address -fno-omit-frame-pointer -Wno-error' --enable-debug
```

My command line is:
./ffmpeg -i input_file

Make sure you don't have a file named au_to0.ts, It suppose to fail while trying to open it.

I compiled with various compilers and this specific input file with clang6.0 and ran the binary in Ubuntu 18.04.

comment:4 by Steven Liu, 3 years ago

follow-up: 5

try this patch please:

<https://patchwork.ffmpeg.org/project/ffmpeg/patch/20200516121156.81344-1-lq@chinaffmpeg.org/>

comment:5 by Assaf Sion, 3 years ago

in reply to: 4 ; follow-up: 6

Replying to [stevenliu](#):

try this patch please:

<https://patchwork.ffmpeg.org/project/ffmpeg/patch/20200516121156.81344-1-lq@chinaffmpeg.org/>

No crash with this patch.

comment:6 by Steven Liu, 3 years ago

in reply to: 5

Replying to [assafsion](#):

Replying to [stevenliu](#):

try this patch please:

<https://patchwork.ffmpeg.org/project/ffmpeg/patch/20200516121156.81344-1-lq@chinaffmpeg.org/>

No crash with this patch.

Maybe this patch is better than the previous patch.

<https://patchwork.ffmpeg.org/project/ffmpeg/patch/20200529033905.41926-1-lq@chinaffmpeg.org/>

comment:7 by Assaf Sion, 3 years ago

Cc: assafsion@gmail.com added

Owner: changed from Assaf Sion to Steven Liu

comment:8 by Assaf Sion, 3 years ago

You can mark the issue as fixed once the patch is in.

comment:9 by Assaf Sion, 3 years ago

Do you have a planned release date?

comment:10 by Assaf Sion, 3 years ago

This was assigned with CVE-2020-13904

comment:11 by Steven Liu, 3 years ago

Resolution: → fixed

Status: open → closed

fixed by commit: [9dfb19baeb86a8bb02c53a441682c6e9a6e104cc](#)

Note: See [TracTickets](#) for help on using tickets.

