

New issue

[Jump to bottom](#)

Bug in ass_outline.c:1354: _Bool outline_stroke(ASS_Outline *, ASS_Outline *, const ASS_Outline *, int, int, int): Assertion `rad >= eps' failed. #431

🔒 Closed F-ZhaoYang opened this issue on Sep 26, 2020 · 9 comments · Fixed by #432

F-ZhaoYang commented on Sep 26, 2020 • edited

fuzzer & poc
[libass.zip](#)

gdb:

```
fstark@fstark-virtual-machine:~/libass$ gdb ./libass_fuzzer
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./libass_fuzzer...done.
(gdb) r out/fuzz5/crashes/id:000000,sig:06,src:000046+000020,time:11326439,op:splice,rep:128
Starting program: /home/fstark/libass/libass_fuzzer out/fuzz5/crashes/id:000000,sig:06,src:000046+000020,time:11326439,op:splice,rep:128
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
***** INFO *****
This binary is built for AFL-fuzz.
To run the target function on individual input(s) execute this:
/home/fstark/libass/libass_fuzzer < INPUT_FILE
or
/home/fstark/libass/libass_fuzzer INPUT_FILE1 [INPUT_FILE2 ... ]
To fuzz with afl-fuzz execute this:
afl-fuzz [afl-flags] /home/fstark/libass/libass_fuzzer [-N]
afl-fuzz will run N iterations before re-spawning the process (default: 1000)
*****
Reading 11249 bytes from out/fuzz5/crashes/id:000000,sig:06,src:000046+000020,time:11326439,op:splice,rep:128
libass_fuzzer: ass_outline.c:1354: _Bool outline_stroke(ASS_Outline *, ASS_Outline *, const ASS_Outline *, int, int, int): Assertion `rad >= eps' failed.

Program received signal SIGABRT, Aborted.
0x00007ffff6efa428 in __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:54
(gdb) t
[Current thread is 1 (Thread 0x7ffff7fdb780 (LWP 25974))]
(gdb) bt
#0 0x00007ffff6efa428 in __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:54
#1 0x00007ffff6efc02a in __GI_abort () at abort.c:89
#2 0x00007ffff6ef2bd7 in __assert_fail_base (fmt=<optimized out>,
assertion=assertion@entry=0x66d940 <str.3> "rad >= eps",
file=file@entry=0x66d820 <str.1> "ass_outline.c", line=line@entry=1354,
function=function@entry=0x66d980 <PRETTY_FUNCTION__outline_stroke> "_Bool outline_stroke(ASS_Outline *, ASS_Outline *, const ASS_Outline *, int, int, int)" ) at assert.c:92
#3 0x00007ffff6ef2c82 in __GI__assert_fail (assertion=0x66d940 <str.3> "rad >= eps",
file=0x66d820 <str.1> "ass_outline.c", line=1354,
function=0x66d980 <PRETTY_FUNCTION__outline_stroke> "_Bool outline_stroke(ASS_Outline *, ASS_Outline *, const ASS_Outline *, int, int, int)" ) at assert.c:101
#4 0x00000000050911f in outline_stroke () at ass_outline.c:1354
#5 0x00000000004de968 in ass_outline_construct () at ass_renderer.c:1222
#6 0x00000000052327d in ass_cache_get () at ass_cache.c:404
#7 0x00000000004f2bb8 in get_bitmap_glyph () at ass_renderer.c:1456
#8 0x00000000004ed5db in render_and_combine_glyphs () at ass_renderer.c:2359
#9 0x00000000004e39e9 in ass_renderer_event () at ass_renderer.c:2787
#10 0x00000000004e17d7 in ass_renderer_frame () at ass_renderer.c:3153
#11 0x00000000004cc94d in LLVMFuzzerTestOneInput () at /src/libass_fuzzer.cc:45
#12 0x00000000004ccf5f in ExecuteFilesOnByOne () at /src/libfuzzer/afl/afl_driver.cpp:217
#13 main () at /src/libfuzzer/afl/afl_driver.cpp:254
```

astiob commented on Sep 26, 2020

Member

@MrSmile Will you take a look?

TheOneric commented on Sep 26, 2020 • edited

Member

In `ass_outline_construct`'s call to `outline_stroke` a signed integer overflow happens *(undefined behaviour)*. On my machine signed overflow happens to wrap around to a negative value, thus failing the assert.

#261 does currently not prevent this overflow .

...

```
ass_renderer.c:1222:18: runtime error: signed integer overflow: 189629639 * 16 cannot be represented in type 'int'
ass_renderer.c:1222:18: runtime error: signed integer overflow: 189629639 * 16 cannot be represented in type 'int'
fuzz: ass_outline.c:1354: outline_stroke: Assertion `rad >= eps' failed.
...
```

 MrSmile mentioned this issue on Sep 26, 2020

Fix overflows in outline processing #432



hyder365 commented on Sep 29, 2020

Any chance of a new release with this fix? The patch doesn't apply to 1.14.0

kaplan-michael commented on Oct 5, 2020

Hey folks, wondering if this will get a CVE?
I think it should. Could someone possibly request it from Mitre? [<https://cveform.mitre.org/>]

F-ZhaoYang commented on Oct 5, 2020

Author

Hey folks, wondering if this will get a CVE?
I think it should. Could someone possibly request it from Mitre? [<https://cveform.mitre.org/>]

Hello, I really don't know how to apply for CVE, I see the announcement seems to require the project manager to issue security advice.
<https://docs.github.com/en/free-pro-team@latest/github/managing-security-vulnerabilities/about-github-security-advisories>
If possible, I hope to apply for a CVE, thank you.

kaplan-michael commented on Oct 5, 2020

Hey,

Hello, I really don't know how to apply for CVE, I see the announcement seems to require the project manager to issue security advice.
<https://docs.github.com/en/free-pro-team@latest/github/managing-security-vulnerabilities/about-github-security-advisories>
If possible, I hope to apply for a CVE, thank you.

I can help with that if you need to. You can request one directly from Mitre, the link i shared earlier.
Or possibly better approach here would be to use GitHub Security Advisories and request it there.

 astiob closed this as completed in [676f9dc](#) on Oct 8, 2020

Foxboron commented on Oct 9, 2020

Hi.

Since this project is on github you can use the security advisory feature to request a CVE.
<https://github.com/libass/libass/security/advisories>

Else using the form works as well.



 anthraxx mentioned this issue on Oct 9, 2020

Release 0.15.0 #341



F-ZhaoYang commented on Oct 9, 2020

Author

Hi.
Since this project is on github you can use the security advisory feature to request a CVE.
<https://github.com/libass/libass/security/advisories>
Else using the form works as well.

Think you , but I can only directly contact maintainers to ask them to create security advisories or issue CVEs on my behalf in repositories that i'm not administer.

F-ZhaoYang commented on Mar 2, 2021

Author

This is [CVE-2020-26682](#)

 MingcongBai mentioned this issue on Mar 29, 2021

libass: Overflows in Outline Processing AOSC-Dev/aosc-os-abbs#2928



 TheOneric mentioned this issue on Apr 12

Negative Fontsize: assert fail in outline_stroke #610



No one assigned

Labels

None yet

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Fix overflows in outline processing**
MrSmile/libass

6 participants

