

## Instantly share code, notes, and snippets.

Criticayon / [CVE-2026-30656.md](#) Secret

Created last week

[Code](#) [Revisions](#) 1

Reference for CVE-2026-30656

[CVE-2026-30656.md](#)

**Description of the bug:** fio crashes when parsing a job file that contains the fdp\_pli option without a value. The parser passes input = NULL to the callback function str\_fdp\_pli\_cb, which then calls strdup(input) without validation, causing a segmentation fault. This is a parser robustness issue. While not a security vulnerability under default CLI usage, it could lead to denial-of-service if fio is used as a backend service processing untrusted job files.

**[VulnerabilityType Other]** NULL Pointer Dereference (CWE-476)

**[Vendor of Product]** fio project (axboe/fio)

**[Affected Product Code Base]** fio (Flexible I/O Tester) - Affected: fio-3.41(commit a8ab726842f4140dfcdb4240138f1abba9b54c05 and earlier) Fixed: fio-3.41(commit 9387e61b5fcfbce1e4ed29b0cd19890a37ba1766)

**[Affected Component]** options.c, str\_fdp\_pli\_cb(), fio job file parser, fdp\_pli option handler

**[Attack Type]** Local

**Environment:** Ubuntu 24.04.3 LTS

**Reproduction steps** Create a minimal job file crash.fio with the following content:

```
[write-heavy]
fdp_pli
```

Run:

```
./fio crash.fio
```

## Observed result:

```

⊗ [AFL++ 8ba3c61bcc1] /home/fuzz_fio # /home/fuzz_fio/fio-src/fio /home/fuzz_fio/test/poc.fio
Segmentation fault (core dumped)
⊙ [AFL++ 8ba3c61bcc1] /home/fuzz_fio # []

```

## GDB backtrace:

```

(gdb) bt
#0  __strlen_evex () at ../sysdeps/x86_64/multiarch/strlen-evex-base.S:81
#1  0x00007fb8351c353 in  __GI__strdup (s=s@entry=0x0) at ./string/strdup.c:41
#2  0x0000560d2aaf5851 in  str_fdp_pli_cb (data=data@entry=0x7fbe7b060028, input=input@entry=0x0) at options.c:269
#3  0x0000560d2a9aa883 in  __handle_option (o=0x560d2abf1980 <fio_options+187488>, ptr=<optimized out>, data=0x7fbe7b060028, curr=<optimized out>, first=<optimized out>, more=<optimized out>) at parse.c:602
#4  handle_option (o=0x560d2abf1980 <fio_options+187488>, __ptr=_ptr@entry=0x0, data=data@entry=0x7fbe7b060028) at parse.c:1056
#5  0x0000560d2aaed5b3 in  parse_option (opt=opt@entry=0x560d55816950 "fdp_pli", input=0x560d55816910 "fdp_pli", options=options@entry=0x560d2abc3d20 <fio_options>, o=c@entry=0x7ffe94c35150, data=data@entry=0x7fbe7b060028, dump_list=dump_list@entry=0x7fbe7b060010) at parse.c:1226
#6  0x0000560d2aaf8e96 in  fio_options_parse (td=td@entry=0x7fbe7b060010, opts=0x560d55813750, num_opts=1) at options.c:5970
#7  0x0000560d2aa9707c in  __parse_jobs_ini (td=0x7fbe7b060010, td@entry=0x0, file=0x560d558136b0 "/home/fuzz_fio/test/crash.fio", is_buf=is_buf@entry=0, stonewall_flag=stonewall_flag@entry=0, type=type@entry=1, nested=nested@entry=0, name=<optimized out>, popts=<optimized out>, aopts=<optimized out>, nopts=<optimized out>) at init.c:2279
#8  0x0000560d2aa9b5e6 in  parse_jobs_ini (file=0x0, is_buf=0, stonewall_flag=0, type=1) at init.c:2334
#9  parse_options (argc=argc@entry=2, argv=argv@entry=0x7ffe94c35468) at init.c:3215
#10 0x0000560d2ab37cfe in  main (argc=2, argv=0x7ffe94c35468, envp=<optimized out>) at fio.c:36
(gdb) []

```

## Notes:

Discovered via AFL++ fuzzing.

Minimal reproducer provided above.