New issue

Segmentation fault in str_fdp_pli_cb when fdp_pli option has no value #2055

Closed

Criticayon opened on Feb 8 Contributor

Please acknowledge the following before creating a ticket

- [x] I have read the GitHub issues section of REPORTING-BUGS.

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.

Environment: Ubuntu 24.04.3 LTS

fio version: fio-3.41

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

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

Run:

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

Observed result:

```
[AFL++ 8ba3c61bccc1] /home/fuzz_fio # /home/fuzz_fio/fio-src/fio /home/fuzz_fio/test/crash.fio
Segmentation fault (core dumped)
```

GDB backtrace:

```
(gdb) bt
#0  __strlen_evex () at ../sysdeps/x86_64/multiarch/strlen-evex-base.S:81
#1  0x00007fbe8351c353 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  0x0000560d2aaea883 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=o@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 0x0000560d2ab87cfe in main (argc=2, argv=0x7ffe94c35468, envp=<optimized out>) at fio.c:36
```

Suggested fix:

Add a NULL check at the start of the callback function str_fdp_pli_cb,eg:

```
if (!input)
    return 1;
p = str = strdup(input);
```

This ensures the parser does not crash when the fdp_pli option is present without a value.

Notes:

Discovered via AFL++ fuzzing.

Minimal reproducer provided above.

axboe added a commit that references this issue on Feb 8

`parse: check for NULL input` … `9387e61`

axboe on Feb 8 — Owner

Thanks, wonder how that survived so long. The real fix is to handle it in the parser, as this issue isn't specific to just that one option. Pushed a fix, closing this one up.

axboe closed this as completed on Feb 8

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants