New issue

Jump to bottom

Floating point exception on Mach-O parser #18667

Closed **CT-Zer0** opened this issue on May 7, 2021 · 1 comment

CT-Zer0 commented on May 7, 2021 • edited

Environment

```
fuzz@fuzz:~/fuzz/issue$ date
Fri 07 May 2021 01:44:26 PM UTC
fuzz@fuzz:~/fuzz/issue$ r2 -v
radare2 5.3.0-git 26142 @ linux-x86-64 git.5.2.1
commit: 518bf6664cedcb3035c9c47388b4fa03bba66748 build: 2021-05-07__12:55:47
fuzz@fuzz:~/fuzz/issue$ uname -ms
Linux x86_64
```

Description

While I am fuzzing rabin2 binary with -I parameter, I found out that there may be a floating point exception (divide by zero) bug on it. rebase_buffer function is throwing floating point exception with the attached Mach-O file. I am not debugging master but page_size is 0 on rebase_buffer which may cause to this bug.
With MSAN:

```
fuzz@fuzz:~/fuzz/issue$ rabin2 -I test
MemorySanitizer:DEADLYSIGNAL
==905482==ERROR: MemorySanitizer: FPE on unknown address 0x7ffff3ed678c (pc 0x7ffff3ed678c bp 0x7fffffff988c0 sp 0x7fffffff98470 T905482)
    #0 0x7ffff3ed678c in rebase_buffer /home/fuzz/fuzz/radare2/libr/../libr/bin/p/bin_mach0.c:778:49
    #1 0x7ffff3ed5b71 in rebasing_and_stripping_io_read /home/fuzz/fuzz/radare2/libr/../libr/bin/p/bin_mach0.c:757:3
    #2 0x7ffff791acf7 in r_io_plugin_read /home/fuzz/fuzz/radare2/libr/io/io_plugin.c:162:9
    #3 0x7ffff792cc03 in r_io_desc_read /home/fuzz/fuzz/radare2/libr/io/io_desc.c:205:12
    #4 0x7ffff794baa5 in r_io_fd_read /home/fuzz/fuzz/radare2/libr/io/io_fd.c:21:15
    #5 0x7ffff74a97ca in buf_io_read /home/fuzz/fuzz/radare2/libr/util/./buf_io.c:72:9
    #6 0x7ffff74981ae in buf_read /home/fuzz/fuzz/radare2/libr/util/buf.c:40:27
    #7 0x7ffff7495e77 in r_buf_read /home/fuzz/fuzz/radare2/libr/util/buf.c:427:11
    #8 0x7ffff749512b in r_buf_read_at /home/fuzz/fuzz/radare2/libr/util/buf.c:577:6
    #9 0x7ffff3f13412 in get_hdr /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/mach0/mach0.c:4343:8
    #10 0x7ffff3f16d81 in mach_fields /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/mach0/mach0.c:4224:35
    #11 0x7ffff3c3d9be in r_bin_object_set_items /home/fuzz/fuzz/radare2/libr/bin/bobj.c:313:15
    #12 0x7ffff3c3b588 in r_bin_object_new /home/fuzz/fuzz/radare2/libr/bin/bobj.c:172:2
    #13 0x7ffff3c1d379 in r_bin_file_new_from_buffer /home/fuzz/fuzz/radare2/libr/bin/bfile.c:529:19
    #14 0x7ffff3bb803b in r_bin_open_buf /home/fuzz/fuzz/radare2/libr/bin/bin.c:286:8
    #15 0x7ffff3bb6048 in r_bin_open_io /home/fuzz/fuzz/radare2/libr/bin/bin.c:346:13
    #16 0x7ffff3bb4919 in r_bin_open /home/fuzz/fuzz/radare2/libr/bin/bin.c:231:9
    #17 0x7ffff7dde246 in r_main_rabin2 /home/fuzz/fuzz/radare2/libr/main/rabin2.c:1069:7
    #18 0x5555555ec931 in main /home/fuzz/fuzz/radare2/binr/rabin2/rabin2.c:6:9
    #19 0x7ffff7bb10b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
    #20 0x55555557225d in _start (/home/fuzz/fuzz/radare2/binr/rabin2/rabin2+0x1e25d)

MemorySanitizer can not provide additional info.
SUMMARY: MemorySanitizer: FPE /home/fuzz/fuzz/radare2/libr/../libr/bin/p/bin_mach0.c:778:49 in rebase_buffer
==905482==ABORTING
```

Without ASAN:

```
fuzz@fuzz:~/fuzz/issue$ rabin2 -I test
Floating point exception
```

This issue is also produced with radare2:

```
fuzz@fuzz:~/fuzz/issue$ radare2 floating_point
Floating point exception
```

Test

Value of page_size variable when `ut64 page_idx = (R_MAX (start, off) - start) / page_size;` is called.

```
fuzz@fuzz:~/fuzz/issue$ gdb rabin2
GNU gdb (Ubuntu 9.2-0ubuntu1~20.04) 9.2
Copyright (C) 2020 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 rabin2...
(gdb) r -I test
Starting program: /usr/local/bin/rabin2 -I test
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGFPE, Arithmetic exception.
0x00007ffff3ed678c in rebase_buffer (obj=0x717000000700, off=0, fd=0x704000005a80, buf=0x70200002eea0 "\376\355\372\316", <incomplete sequence \362>, count=28)
    at /home/fuzz/fuzz/radare2/libr/../libr/bin/p/bin_mach0.c:778
778                             ut64 page_idx = (R_MAX (start, off) - start) / page_size;
(gdb) p page_size
$1 = 0
(gdb) p start
$2 = 25
(gdb)
```

File format of test file.

```
fuzz@fuzz:~/fuzz/issue$ file floating_point
floating_point: Mach-O architecture=65535 filetype=738197504, flags:<|INCRLINK>
fuzz@fuzz:~/fuzz/issue$
```

floating_point.zip

trufae commented on May 7, 2021 — Contributor

Thanks! fixed

trufae closed this as completed in a07dedb on May 7, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants