New issue

Jump to bottom

Heap memory bugs on pyc parse #18679

Closed CT-Zer0 opened this issue on May 11, 2021 · 2 comments

CT-Zer0 commented on May 11, 2021

Environment

```
# copypaste this script into your shell and replace it with the output
fuzz@fuzz:~/fuzz/issue$ date
Tue 11 May 2021 11:50:43 AM UTC
fuzz@fuzz:~/fuzz/issue$ r2 -v
radare2 5.3.0-git 26277 @ linux-x86-64 git.5.2.1
commit: 708e5c986ce686b01b84a6162f1cec1429ea8198 build: 2021-05-11__09:03:45
fuzz@fuzz:~/fuzz/issue$ uname -ms
Linux x86_64
```

Description

While I am fuzzing rabin2 with -I parameter, I am encountered several heap memory bugs with the same file on different sanitizers. I assume that if nested pyc magic byte (94 94 94) is occured in file, radare2 tries to parse and does memory operations more than once and heap memory bugs are triggered. While ASAN throws heap-use-after free error on r_bin_object_set_items, MSAN and vanilla run throws double-free error. This will lead seperate bugs both on r_bin_filter_name and r_bin_object_set_items .

With ASAN:

```
fuzz@fuzz:~/fuzz/issue$ rabin2 -I heap-use-after-free
Undefined type in get_object (0x7e)
Copy not implemented for type 66
Undefined type in get_object (0x7f)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
=================================================================
==1118949==ERROR: AddressSanitizer: heap-use-after-free on address 0x60700007e200 at pc 0x7ffff41b0064 bp 0x7fffffff9c3f0 sp 0x7fffffff9c3e0
READ of size 8 at 0x60700007e200 thread T0
    #0 0x7ffff41b0063 in r_bin_object_set_items /home/fuzz/fuzz/radare2/libr/bin/bobj.c:345
    #1 0x7ffff41ae3ac in r_bin_object_new /home/fuzz/fuzz/radare2/libr/bin/bobj.c:172
    #2 0x7ffff41a8c1d in r_bin_file_new_from_buffer /home/fuzz/fuzz/radare2/libr/bin/bfile.c:529
    #3 0x7ffff4187532 in r_bin_open_buf /home/fuzz/fuzz/radare2/libr/bin/bin.c:286
    #4 0x7ffff4187bb9 in r_bin_open_io /home/fuzz/fuzz/radare2/libr/bin/bin.c:346
    #5 0x7ffff4186a72 in r_bin_open /home/fuzz/fuzz/radare2/libr/bin/bin.c:231
    #6 0x7ffff7549e8b in r_main_rabin2 /home/fuzz/fuzz/radare2/libr/main/rabin2.c:1069
    #7 0x5555555551ac in main /home/fuzz/fuzz/radare2/binr/rabin2/rabin2.c:6
    #8 0x7ffff73520b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #9 0x5555555550cd in _start (/home/fuzz/fuzz/radare2/binr/rabin2/rabin2+0x10cd)

0x60700007e200 is located 32 bytes inside of 72-byte region [0x60700007e1e0,0x60700007e228)
freed by thread T0 here:
    #0 0x7ffff769b7cf in __interceptor_free (/lib/x86_64-linux-gnu/libasan.so.5+0x10d7cf)
    #1 0x7ffff442b45b in extract_sections_symbols /home/fuzz/fuzz/radare2/libr/..//libr/bin/p/../format/pyc/marshal.c:1205
    #2 0x7ffff442b4f7 in get_sections_symbols_from_code_objects /home/fuzz/fuzz/radare2/libr/..//libr/bin/p/../format/pyc/marshal.c:1218
    #3 0x7ffff442c18c in pyc_get_sections_symbols /home/fuzz/fuzz/radare2/libr/..//libr/bin/p/../format/pyc/pyc.c:7
    #4 0x7ffff4423c07 in symbols /home/fuzz/fuzz/radare2/libr/..//libr/bin/p/bin_pyc.c:124
    #5 0x7ffff41afbd2 in r_bin_object_set_items /home/fuzz/fuzz/radare2/libr/bin/bobj.c:327
    #6 0x7ffff41ae3ac in r_bin_object_new /home/fuzz/fuzz/radare2/libr/bin/bobj.c:172
    #7 0x7ffff41a8c1d in r_bin_file_new_from_buffer /home/fuzz/fuzz/radare2/libr/bin/bfile.c:529
    #8 0x7ffff4187532 in r_bin_open_buf /home/fuzz/fuzz/radare2/libr/bin/bin.c:286
    #9 0x7ffff4187bb9 in r_bin_open_io /home/fuzz/fuzz/radare2/libr/bin/bin.c:346
    #10 0x7ffff4186a72 in r_bin_open /home/fuzz/fuzz/radare2/libr/bin/bin.c:231
    #11 0x7ffff7549e8b in r_main_rabin2 /home/fuzz/fuzz/radare2/libr/main/rabin2.c:1069
    #12 0x5555555551ac in main /home/fuzz/fuzz/radare2/binr/rabin2/rabin2.c:6
    #13 0x7ffff73520b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

previously allocated by thread T0 here:
    #0 0x7ffff769bdc6 in calloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10ddc6)
    #1 0x7ffff442adf4 in extract_sections_symbols /home/fuzz/fuzz/radare2/libr/..//libr/bin/p/../format/pyc/marshal.c:1166
    #2 0x7ffff442b4f7 in get_sections_symbols_from_code_objects /home/fuzz/fuzz/radare2/libr/..//libr/bin/p/../format/pyc/marshal.c:1218
    #3 0x7ffff442c18c in pyc_get_sections_symbols /home/fuzz/fuzz/radare2/libr/..//libr/bin/p/../format/pyc/pyc.c:7
    #4 0x7ffff4423c07 in symbols /home/fuzz/fuzz/radare2/libr/..//libr/bin/p/bin_pyc.c:124
    #5 0x7ffff41afbd2 in r_bin_object_set_items /home/fuzz/fuzz/radare2/libr/bin/bobj.c:327
    #6 0x7ffff41ae3ac in r_bin_object_new /home/fuzz/fuzz/radare2/libr/bin/bobj.c:172
    #7 0x7ffff41a8c1d in r_bin_file_new_from_buffer /home/fuzz/fuzz/radare2/libr/bin/bfile.c:529
    #8 0x7ffff4187532 in r_bin_open_buf /home/fuzz/fuzz/radare2/libr/bin/bin.c:286
    #9 0x7ffff4187bb9 in r_bin_open_io /home/fuzz/fuzz/radare2/libr/bin/bin.c:346
    #10 0x7ffff4186a72 in r_bin_open /home/fuzz/fuzz/radare2/libr/bin/bin.c:231
    #11 0x7ffff7549e8b in r_main_rabin2 /home/fuzz/fuzz/radare2/libr/main/rabin2.c:1069
    #12 0x5555555551ac in main /home/fuzz/fuzz/radare2/binr/rabin2/rabin2.c:6
    #13 0x7ffff73520b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/fuzz/radare2/libr/bin/bobj.c:345 in r_bin_object_set_items
Shadow bytes around the buggy address:
  0x0c0e80007bf0: fd fd fa fa fa fa 00 00 00 00 00 00 00 00 00 00
  0x0c0e80007c00: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c0e80007c10: fa fa fd fd fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0e80007c20: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fd fd
  0x0c0e80007c30: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
=>0x0c0e80007c40:[fd]fd fd fd fd fa fa fa fa 00 00 00 00 00 00
  0x0c0e80007c50: 00 00 04 fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e80007c60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e80007c70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e80007c80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e80007c90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 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
  Shadow gap:              cc
==1118949==ABORTING
```

With MSAN:

```
fuzz@fuzz:~/fuzz/issue/11-may$ rabin2 -I heap-use-after-free
Undefined type in get_object (0x7e)
Copy not implemented for type 66
Undefined type in get_object (0x7f)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
MemorySanitizer:DEADLYSIGNAL
==1689666==ERROR: MemorySanitizer: SEGV on unknown address (pc 0x7ffff7c3ed5a bp 0x7fffffff99180 sp 0x7fffffff98c08 T1689666)
==1689666==The signal is caused by a READ memory access.
==1689666==Hint: this fault was caused by a dereference of a high value address (see register values below).  Dissassemble the provided pc to learn which register was used.
    #0 0x7ffff7c3ed5a  /build/glibc-eX1tMB/glibc-2.31/string/../sysdeps/x86_64/multiarch/../strlen.S:120
    #1 0x7ffff7c05e94 in __vfprintf_internal /build/glibc-eX1tMB/glibc-2.31/stdio-common/vfprintf-internal.c:1688:4
    #2 0x7ffff7c19119 in __vsnprintf_internal /build/glibc-eX1tMB/glibc-2.31/libio/vsnprintf.c:114:9
    #3 0x555555587961 in vsnprintf (/home/fuzz/fuzz/radare2/binr/rabin2/rabin2+0x33961)
    #4 0x7ffff77b2244 in sdb_fmt /home/fuzz/fuzz/radare2/shlr/sdb/src/fmt.c:33:3
    #5 0x7ffff3c0f6a8 in r_bin_filter_name /home/fuzz/fuzz/radare2/libr/bin/filter.c:36:22
    #6 0x7ffff3c12aa1 in r_bin_filter_sections /home/fuzz/fuzz/radare2/libr/bin/filter.c:135:13
    #7 0x7ffff3c3d6f1 in r_bin_object_set_items /home/fuzz/fuzz/radare2/libr/bin/bobj.c:347:4
    #8 0x7ffff3c39588 in r_bin_object_new /home/fuzz/fuzz/radare2/libr/bin/bobj.c:172:2
    #9 0x7ffff3c1b379 in r_bin_file_new_from_buffer /home/fuzz/fuzz/radare2/libr/bin/bfile.c:529:19
    #10 0x7ffff3bb603b in r_bin_open_buf /home/fuzz/fuzz/radare2/libr/bin/bin.c:286:8
    #11 0x7ffff3bb4048 in r_bin_open_io /home/fuzz/fuzz/radare2/libr/bin/bin.c:346:13
    #12 0x7ffff3bb2919 in r_bin_open /home/fuzz/fuzz/radare2/libr/bin/bin.c:231:9
    #13 0x7ffff7dde246 in r_main_rabin2 /home/fuzz/fuzz/radare2/libr/main/rabin2.c:1069:7
    #14 0x5555555ec931 in main /home/fuzz/fuzz/radare2/binr/rabin2/rabin2.c:6:9
    #15 0x7ffff7bb10b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
    #16 0x555555557225d in _start (/home/fuzz/fuzz/radare2/binr/rabin2/rabin2+0x1e25d)

MemorySanitizer can not provide additional info.
SUMMARY: MemorySanitizer: SEGV /build/glibc-eX1tMB/glibc-2.31/string/../sysdeps/x86_64/multiarch/../strlen.S:120
==1689666==ABORTING
```

Without sanitizer:

```
fuzz@fuzz:~/fuzz/issue/11-may$ rabin2 -I heap-use-after-free
Undefined type in get_object (0x7e)
Copy not implemented for type 66
Undefined type in get_object (0x7f)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
free(): double free detected in tcache 2
Aborted
```

Although, When I will test it with nested 94 94 94 with no following bytes, It runs normally.

```
fuzz@fuzz:~/fuzz/issue/11-may$ rabin2 -I test-without-nested
Undefined type in get_object (0x7e)
Copy not implemented for type 66
Undefined type in get_object (0x7f)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Free not implemented for type 7b
Free not implemented for type 66
arch     pyc
cpu      0.9.4 beta
baddr    0x0
binsz    40
bintype  pyc
bits     16
canary   false
retguard false
class    Python byte-compiled file
crypto   false
endian   little
havecode true
laddr    0x0
linenum  false
lsyms    false
machine  Python 0.9.4 beta VM (rev 77b80a91d357c1d95d8e7cd4cbbe799e5deb777e)
maxopsz  16
minopsz  1
nx       false
os       any
pcalign  0
pic      false
relocs   false
sanitiz  false
static   true
stripped false
va       false
```

```
fuzz@fuzz:~/fuzz/issue/11-may$ xxd heap-use-after-free
00000000: 9494 9400 948e 6400 6387 2040 9440 0024  ......d.c. @.@.$
00000010: eb10 2015 ff7f 0000 107b fee6 00ff fa00  .. ......{......
00000020: 9494 94fa 0094 9494 0094 9494 ff7f 7d7d  ..............}}
00000030: 7f43                                     .C
fuzz@fuzz:~/fuzz/issue/11-may$ xxd test-without-nested
00000000: 9494 9400 945e 6400 6387 2040 9440 0024  .....^d.c. @.@.$
00000010: eb10 2015 ff7f 0000 107b fee6 00ff fa00  .. ......{......
00000020: 9494 94fa 0094 9494                      ........
fuzz@fuzz:~/fuzz/issue/11-may$ rabin2 -I test-without-nested
Undefined type in get_object (0x7e)
Copy not implemented for type 66
Undefined type in get_object (0x7f)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Free not implemented for type 7b
Free not implemented for type 66
arch     pyc
cpu      0.9.4 beta
baddr    0x0
binsz    40
bintype  pyc
bits     16
canary   false
retguard false
class    Python byte-compiled file
crypto   false
endian   little
havecode true
laddr    0x0
linenum  false
lsyms    false
machine  Python 0.9.4 beta VM (rev 77b80a91d357c1d95d8e7cd4cbbe799e5deb777e)
maxopsz  16
minopsz  1
nx       false
os       any
pcalign  0
pic      false
relocs   false
sanitiz  false
static   true
stripped false
va       false
fuzz@fuzz:~/fuzz/issue/11-may$
```

It is failing with additional bytes after nested magic byte.

```
fuzz@fuzz:~/fuzz/issue/11-may$ xxd test-with-additional-byte
00000000: 9494 9400 945e 6400 6387 2040 9440 0024  .....^d.c. @.@.$
00000010: eb10 2015 ff7f 0000 107b fee6 00ff fa00  .. ......{......
00000020: 9494 94fa 0094 9494 a0                   .........
fuzz@fuzz:~/fuzz/issue/11-may$ rabin2 -I test-with-additional-byte
Undefined type in get_object (0x7e)
Copy not implemented for type 66
Undefined type in get_object (0x7f)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
Undefined type in get_object (0x14)
free(): double free detected in tcache 2
Aborted
fuzz@fuzz:~/fuzz/issue/11-may$
```

Test

You can find files mentioned above in this zip file.

heap-use-after-free.zip

1

radare added a commit to radareorg/radare2-testbins that referenced this issue on May 11, 2021

`Add testbins from radareorg/radare2#18679` `77e5771`

trufae closed this as completed in `049de62` on May 11, 2021

---

trufae commented on May 11, 2021 — Contributor

Thanks! that's a good catch. it's now fixed in master

ajakk mentioned this issue on May 16, 2021

use-after-free in pyc parsing rizinorg/rizin#1137

Closed

CT-Zer0 commented on May 25, 2021 — Author

CVE-2021-32613 is assigned for this issue.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants