New issue

Jump to bottom

Heap-use-after-free bug on .pyc parser #18666

Closed **CT-Zer0** opened this issue on May 7, 2021 · 0 comments

CT-Zer0 commented on May 7, 2021 • edited

Environment

```
fuzz@fuzz:~/fuzz$ date
Fri 07 May 2021 12:59:49 PM UTC
fuzz@fuzz:~/fuzz$ 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$ uname -ms
Linux x86_64
```

Description

While I am fuzzing rabin2 binary with -I parameter, I found out that there may be a heap-use-after-free (and double-free , I guess) bug on it. I am suspecting that two same undefined types are found and rabin2 tries to manipulate (copy, free etc) without control.

With MSAN:

```
 fuzz@fuzz:~/fuzz/issue$ rabin2 -I double_free
Copy not implemented for type 78
==899274==WARNING: MemorySanitizer: use-of-uninitialized-value
    #0 0x7ffff43be235 in free_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:721:6
    #1 0x7ffff43bdcf9 in get_code_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:978:3
    #2 0x7ffff43c17c9 in get_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1065:9
    #3 0x7ffff43bec47 in get_sections_symbols_from_code_objects /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1218:34
    #4 0x7ffff43cf3d1 in pyc_get_sections_symbols /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/pyc.c:7:9
    #5 0x7ffff43ba51e in symbols /home/fuzz/fuzz/radare2/libr/../libr/bin/p/bin_pyc.c:124:2
    #6 0x7ffff3c3e446 in r_bin_object_set_items /home/fuzz/fuzz/radare2/libr/bin/bobj.c:327:16
    #7 0x7ffff3c3b588 in r_bin_object_new /home/fuzz/fuzz/radare2/libr/bin/bobj.c:172:2
    #8 0x7ffff3c1d379 in r_bin_file_new_from_buffer /home/fuzz/fuzz/radare2/libr/bin/bfile.c:529:19
    #9 0x7ffff3bb803b in r_bin_open_buf /home/fuzz/fuzz/radare2/libr/bin/bin.c:286:8
    #10 0x7ffff3bb6048 in r_bin_open_io /home/fuzz/fuzz/radare2/libr/bin/bin.c:346:13
    #11 0x7ffff3bb4919 in r_bin_open /home/fuzz/fuzz/radare2/libr/bin/bin.c:231:9
    #12 0x7ffff7dde246 in r_main_rabin2 /home/fuzz/fuzz/radare2/libr/main/rabin2.c:1069:7
    #13 0x5555555ec931 in main /home/fuzz/fuzz/radare2/binr/rabin2/rabin2.c:6:9
    #14 0x7ffff7bb10b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
    #15 0x55555557225d in _start (/home/fuzz/fuzz/radare2/binr/rabin2/rabin2+0x1e25d)

SUMMARY: MemorySanitizer: use-of-uninitialized-value /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:721:6 in free_object
Exiting
```

With ASAN:

```
=================================================================
==1631110==ERROR: AddressSanitizer: heap-use-after-free on address 0x602000065890 at pc 0x7fffef7c994c bp 0x7fffffff99320 sp 0x7fffffff99318
READ of size 4 at 0x602000065890 thread T0
    #0 0x7fffef7c994b in copy_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:790:23
    #1 0x7fffef7c1b53 in get_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1141:19
    #2 0x7fffef7bc09e in get_code_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:940:15
    #3 0x7fffef7c1718 in get_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1065:9
    #4 0x7fffef7be85f in get_sections_symbols_from_code_objects /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1218:34
    #5 0x7fffef7ce054 in pyc_get_sections_symbols /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/pyc.c:7:9
    #6 0x7fffef7b985f in symbols /home/fuzz/fuzz/radare2/libr/../libr/bin/p/bin_pyc.c:124:2
    #7 0x7fffef003464 in r_bin_object_set_items /home/fuzz/fuzz/radare2/libr/bin/bobj.c:327:16
    #8 0x7fffeefff4bc in r_bin_object_new /home/fuzz/fuzz/radare2/libr/bin/bobj.c:172:2
    #9 0x7fffeefe4299 in r_bin_file_new_from_buffer /home/fuzz/fuzz/radare2/libr/bin/bfile.c:529:19
    #10 0x7fffeef827c9 in r_bin_open_buf /home/fuzz/fuzz/radare2/libr/bin/bin.c:286:8
    #11 0x7fffeef80381 in r_bin_open_io /home/fuzz/fuzz/radare2/libr/bin/bin.c:346:13
    #12 0x7fffeef7edf0 in r_bin_open /home/fuzz/fuzz/radare2/libr/bin/bin.c:231:9
    #13 0x7ffff7db242b in r_main_rabin2 /home/fuzz/fuzz/radare2/libr/main/rabin2.c:1069:7
    #14 0x555555561af91 in main /home/fuzz/fuzz/radare2/binr/rabin2/rabin2.c:6:9
    #15 0x7ffff7b4d0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
    #16 0x5555555712dd in _start (/home/fuzz/fuzz/radare2/binr/rabin2/rabin2+0x1d2dd)

0x602000065890 is located 0 bytes inside of 16-byte region [0x602000065890,0x6020000658a0)
freed by thread T0 here:
    #0 0x5555555eb0cd in free (/home/fuzz/fuzz/radare2/binr/rabin2/rabin2+0x970cd)
    #1 0x7fffef7be7e9 in free_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:781:2
    #2 0x7fffef7c1b47 in get_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1140:3
    #3 0x7fffef7bc09e in get_code_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:940:15
    #4 0x7fffef7c1718 in get_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1065:9
    #5 0x7fffef7be85f in get_sections_symbols_from_code_objects /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1218:34
    #6 0x7fffef7ce054 in pyc_get_sections_symbols /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/pyc.c:7:9
    #7 0x7fffef7b985f in symbols /home/fuzz/fuzz/radare2/libr/../libr/bin/p/bin_pyc.c:124:2
    #8 0x7fffef003464 in r_bin_object_set_items /home/fuzz/fuzz/radare2/libr/bin/bobj.c:327:16
    #9 0x7fffeefff4bc in r_bin_object_new /home/fuzz/fuzz/radare2/libr/bin/bobj.c:172:2
    #10 0x7fffeefe4299 in r_bin_file_new_from_buffer /home/fuzz/fuzz/radare2/libr/bin/bfile.c:529:19
    #11 0x7fffeef827c9 in r_bin_open_buf /home/fuzz/fuzz/radare2/libr/bin/bin.c:286:8
    #12 0x7fffeef80381 in r_bin_open_io /home/fuzz/fuzz/radare2/libr/bin/bin.c:346:13
    #13 0x7fffeef7edf0 in r_bin_open /home/fuzz/fuzz/radare2/libr/bin/bin.c:231:9
    #14 0x7ffff7db242b in r_main_rabin2 /home/fuzz/fuzz/radare2/libr/main/rabin2.c:1069:7
    #15 0x555555561af91 in main /home/fuzz/fuzz/radare2/binr/rabin2/rabin2.c:6:9
    #16 0x7ffff7b4d0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

previously allocated by thread T0 here:
    #0 0x5555555eb4c2 in calloc (/home/fuzz/fuzz/radare2/binr/rabin2/rabin2+0x974c2)
    #1 0x7fffef7c2376 in get_none_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:93:8
    #2 0x7fffef7c1461 in get_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1022:9
```

```
    #3 0x7fffef7bc09e in get_code_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:940:15
    #4 0x7fffef7c1718 in get_object /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1065:9
    #5 0x7fffef7be85f in get_sections_symbols_from_code_objects /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:1218:34
    #6 0x7fffef7ce054 in pyc_get_sections_symbols /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/pyc.c:7:9
    #7 0x7fffef7b985f in symbols /home/fuzz/fuzz/radare2/libr/../libr/bin/p/bin_pyc.c:124:2
    #8 0x7fffef003464 in r_bin_object_set_items /home/fuzz/fuzz/radare2/libr/bin/bobj.c:327:16
    #9 0x7fffeefff4bc in r_bin_object_new /home/fuzz/fuzz/radare2/libr/bin/bobj.c:172:2
    #10 0x7fffeefe4299 in r_bin_file_new_from_buffer /home/fuzz/fuzz/radare2/libr/bin/bfile.c:529:19
    #11 0x7fffeef827c9 in r_bin_open_buf /home/fuzz/fuzz/radare2/libr/bin/bin.c:286:8
    #12 0x7fffeef80381 in r_bin_open_io /home/fuzz/fuzz/radare2/libr/bin/bin.c:346:13
    #13 0x7fffeef7edf0 in r_bin_open /home/fuzz/fuzz/radare2/libr/bin/bin.c:231:9
    #14 0x7ffff7db242b in r_main_rabin2 /home/fuzz/fuzz/radare2/libr/main/rabin2.c:1069:7
    #15 0x55555561af91 in main /home/fuzz/fuzz/radare2/binr/rabin2/rabin2.c:6:9
    #16 0x7ffff7b4d0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:790:23 in copy_object
Shadow bytes around the buggy address:
  0x0c0480004ac0: fa fa 03 fa fa fa 04 fa fa fa 04 fa fa fa 04 fa
  0x0c0480004ad0: fa fa fd fd fa fa fd fd fa fa 02 fa fa fa 00 04
  0x0c0480004ae0: fa fa fd fd fa fa fd fd fa fa 00 04 fa fa 00 04
  0x0c0480004af0: fa fa 00 04 fa fa 02 fa fa fa fd fa fa fa fd fa
  0x0c0480004b00: fa fa 00 00 fa fa 00 04 fa fa 00 00 fa fa 00 00
=>0x0c0480004b10: fa fa[fd]fd fa fa fd fa fa fa 00 00 fa fa fa fa
  0x0c0480004b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004b30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004b50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004b60: 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
==1631110==ABORTING
```

Without Sanitizer:

```
Undefined type in copy_object (556d8a00)
Copy not implemented for type 78
Undefined type in free_object (556d8a00)
free(): double free detected in tcache 2
Aborted
```

This issue is also produced with radare2:

```
fuzz@fuzz:~/fuzz/issue$ radare2 double_free
Undefined type in copy_object (556b9b50)
Copy not implemented for type 78
Undefined type in free_object (556b9b50)
free(): double free detected in tcache 2
Aborted
```

Test

This is the my debugging screenshot.

```
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) b copy_object
Function "copy_object" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 1 (copy_object) pending.
(gdb) b free_object
Function "free_object" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 2 (free_object) pending.
(gdb) r -I smallest
Starting program: /usr/local/bin/rabin2 -I smallest
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 2, free_object (object=0x5555556b8640) at /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:717
717     static void free_object(pyc_object *object) {
(gdb) c
Continuing.

Breakpoint 2, free_object (object=0x5555556b8830) at /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:717
717     static void free_object(pyc_object *object) {
(gdb) c
Continuing.

Breakpoint 1, copy_object (object=0x7ffff68ed63f <free_object+415>) at /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:784
784     static pyc_object *copy_object(pyc_object *object) {
(gdb) c
Continuing.
Undefined type in copy_object (556b8920)

Breakpoint 2, free_object (object=0x0) at /home/fuzz/fuzz/radare2/libr/../libr/bin/p/../format/pyc/marshal.c:717
717     static void free_object(pyc_object *object) {
(gdb) c
Continuing.
Undefined type in free_object (556b8920)
free(): double free detected in tcache 2

Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
50      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb)
```

double_free.zip

CT-Zer0 changed the title ~~Double-free bug on rabin2~~ Heap-use-after-free bug on rabin2 on May 7, 2021

CT-Zer0 changed the title ~~Heap-use-after-free bug on rabin2~~ Heap-use-after-free bug on marshall.c on May 7, 2021

CT-Zer0 changed the title ~~Heap-use-after-free bug on marshall.c~~ Heap-use-after-free bug on .pyc parser on May 7, 2021

trufae closed this as completed in 5e16e2d on May 7, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant