# Use After Free in op_is_set_bp in radareorg/radare2



Valid Reported on Mar 18th 2022

## Description

Heap use after free in op_is_set_bp function.
ASAN report:

```
=================================================================
==2367298==ERROR: AddressSanitizer: heap-use-after-free on address 0x606000
READ of size 8 at 0x6060000481a0 thread T0
    #0 0x7f580c10da40 in op_is_set_bp /root/radare2/libr/anal/fcn.c:524
    #1 0x7f580c11f8c7 in fcn_recurse /root/radare2/libr/anal/fcn.c:1385
    #2 0x7f580c1211bf in r_anal_function_bb /root/radare2/libr/anal/fcn.c:1
    #3 0x7f580c122e61 in r_anal_function /root/radare2/libr/anal/fcn.c:1554
    #4 0x7f5813218c7a in __core_anal_fcn /root/radare2/libr/core/canal.c:79
    #5 0x7f581322b973 in r_core_anal_fcn /root/radare2/libr/core/canal.c:26
    #6 0x7f5812ebff90 in r_core_af /root/radare2/libr/core/cmd_anal.c:3861
    #7 0x7f581324958d in r_core_anal_all /root/radare2/libr/core/canal.c:42
    #8 0x7f5812f2b8bd in cmd_anal_all /root/radare2/libr/core/cmd_anal.c:11
    #9 0x7f5812f39639 in cmd_anal /root/radare2/libr/core/cmd_anal.c:12223
    #10 0x7f58131fa1c4 in r_cmd_call /root/radare2/libr/core/cmd_api.c:537
    #11 0x7f5813079b67 in r_core_cmd_subst_i /root/radare2/libr/core/cmd.c:
    #12 0x7f5813069a46 in r_core_cmd_subst /root/radare2/libr/core/cmd.c:33
    #13 0x7f58130863a3 in run_cmd_depth /root/radare2/libr/core/cmd.c:5366
    #14 0x7f581308741a in r_core_cmd /root/radare2/libr/core/cmd.c:5449
    #15 0x7f5813088413 in r_core_cmd0 /root/radare2/libr/core/cmd.c:5606
    #16 0x7f581bb2c1d1 in r_main_radare2 /root/radare2/libr/main/radare2.c:
    #17 0x55e8ee37b937 in main /root/radare2/binr/radare2/radare2.c:96
    #18 0x7f581af2c0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #19 0x55e8ee37b30d in _start (/root/radare2/binr/radare2/radare2+0x230d

0x6060000481a0 is located 0 bytes inside of 56-byte region
freed by thread T0 here:
    #0 0x7f581cc7940f in __interceptor_free ../../../../src/libsanitizer/as
```

```
    #0 0x7f581cc7940f in __interceptor_free ../../../../src/libsanitizer/as
    #1 0x7f58081c67de in r_reg_item_free /root/radare2/libr/reg/reg.c:96
    #2 0x7f581c16b32e in r_list_delete /root/radare2/libr/util/list.c:124

    #3 0x7f581c16ade1 in r_list_purge /root/radare2/libr/util/list.c:90
    #4 0x7f581c16afb7 in r_list_free /root/radare2/libr/util/list.c:100
    #5 0x7f58081c7c69 in r_reg_free_internal /root/radare2/libr/reg/reg.c:1
    #6 0x7f58081e099e in r_reg_set_profile_string /root/radare2/libr/reg/pr
    #7 0x7f580c19dded in r_anal_set_reg_profile /root/radare2/libr/anal/ana
    #8 0x7f580c19e663 in r_anal_set_bits /root/radare2/libr/anal/anal.c:324
    #9 0x7f58130a7fbc in cb_asmbits /root/radare2/libr/core/cconfig.c:884
    #10 0x7f581ad45ad7 in r_config_set_i /root/radare2/libr/config/config.c
    #11 0x7f5813128320 in r_core_seek_arch_bits /root/radare2/libr/core/cic
    #12 0x7f5812d4abed in archbits /root/radare2/libr/core/core.c:267
    #13 0x7f580c1014cf in r_anal_op /root/radare2/libr/anal/op.c:110
    #14 0x7f580c108703 in is_delta_pointer_table /root/radare2/libr/anal/fc
    #15 0x7f580c116a37 in fcn_recurse /root/radare2/libr/anal/fcn.c:988
    #16 0x7f580c1211bf in r_anal_function_bb /root/radare2/libr/anal/fcn.c:
    #17 0x7f580c122e61 in r_anal_function /root/radare2/libr/anal/fcn.c:155
    #18 0x7f5813218c7a in __core_anal_fcn /root/radare2/libr/core/canal.c:7
    #19 0x7f581322b973 in r_core_anal_fcn /root/radare2/libr/core/canal.c:2
    #20 0x7f5812ebff90 in r_core_af /root/radare2/libr/core/cmd_anal.c:3861
    #21 0x7f581324958d in r_core_anal_all /root/radare2/libr/core/canal.c:4
    #22 0x7f5812f2b8bd in cmd_anal_all /root/radare2/libr/core/cmd_anal.c:1
    #23 0x7f5812f39639 in cmd_anal /root/radare2/libr/core/cmd_anal.c:12223
    #24 0x7f58131fa1c4 in r_cmd_call /root/radare2/libr/core/cmd_api.c:537
    #25 0x7f5813079b67 in r_core_cmd_subst_i /root/radare2/libr/core/cmd.c:
    #26 0x7f5813069a46 in r_core_cmd_subst /root/radare2/libr/core/cmd.c:33
    #27 0x7f58130863a3 in run_cmd_depth /root/radare2/libr/core/cmd.c:5366
    #28 0x7f581308741a in r_core_cmd /root/radare2/libr/core/cmd.c:5449
    #29 0x7f5813088413 in r_core_cmd0 /root/radare2/libr/core/cmd.c:5606

previously allocated by thread T0 here:
    #0 0x7f581cc79a06 in __interceptor_calloc ../../../../src/libsanitizer/
    #1 0x7f58081dec7b in parse_def /root/radare2/libr/reg/profile.c:68
    #2 0x7f58081e199b in r_reg_set_profile_string /root/radare2/libr/reg/pr
    #3 0x7f580c19dded in r_anal_set_reg_profile /root/radare2/libr/anal/ana
    #4 0x7f580c19e663 in r_anal_set_bits /root/radare2/libr/anal/anal.c:324
    #5 0x7f58130a7fbc in cb_asmbits /root/radare2/libr/core/
    #6 0x7f581ad45ad7 in r_config_set_i /root/radare2/libr/
    #7 0x7f5813128320 in r_core_seek_arch_bits /root/radare2/libr/core/cic
```

```
    #8 0x7f581322afb6 in r_core_anal_fcn /root/radare2/libr/core/canal.c:1
    #9 0x7f5812ebff90 in r_core_af /root/radare2/libr/core/cmd_anal.c:3861
    #10 0x7f581324958d in r_core_anal_all /root/radare2/libr/core/canal.c:4

    #11 0x7f5812f2b8bd in cmd_anal_all /root/radare2/libr/core/cmd_anal.c:1
    #12 0x7f5812f39639 in cmd_anal /root/radare2/libr/core/cmd_anal.c:12223
    #13 0x7f58131fa1c4 in r_cmd_call /root/radare2/libr/core/cmd_api.c:537
    #14 0x7f5813079b67 in r_core_cmd_subst_i /root/radare2/libr/core/cmd.c:
    #15 0x7f5813069a46 in r_core_cmd_subst /root/radare2/libr/core/cmd.c:33
    #16 0x7f58130863a3 in run_cmd_depth /root/radare2/libr/core/cmd.c:5366
    #17 0x7f581308741a in r_core_cmd /root/radare2/libr/core/cmd.c:5449
    #18 0x7f5813088413 in r_core_cmd0 /root/radare2/libr/core/cmd.c:5606
    #19 0x7f581bb2c1d1 in r_main_radare2 /root/radare2/libr/main/radare2.c:
    #20 0x55e8ee37b937 in main /root/radare2/binr/radare2/radare2.c:96
    #21 0x7f581af2c0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.

SUMMARY: AddressSanitizer: heap-use-after-free /root/radare2/libr/anal/fcn.
Shadow bytes around the buggy address:
  0x0c0c80000fe0: fd fd fd fd fd fd fd fa fa fa fa fa fd fd fd fd
  0x0c0c80000ff0: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fa
  0x0c0c80001000: fa fa fa fa fd fd fd fd fd fd fd fa fa fa fa fa
  0x0c0c80001010: fd fd fd fd fd fd fd fa fa fa fa fa fd fd fd fd
  0x0c0c80001020: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fa
=>0x0c0c80001030: fa fa fa fa[fd]fd fd fd fd fd fd fa fa fa fa fa
  0x0c0c80001040: fd fd fd fd fd fd fd fa fa fa fa fa fd fd fd fd
  0x0c0c80001050: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fa
  0x0c0c80001060: fa fa fa fa fd fd fd fd fd fd fd fa fa fa fa fa
  0x0c0c80001070: fd fd fd fd fd fd fd fa fa fa fa fa fd fd fd fd
  0x0c0c80001080: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd 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
==2367298==ABORTING
```

## How can we reproduce the issue?

Compile command

```
./sys/sanitize.sh
```

reproduce command
tests_65185.zip

```
unzip tests_65185.zip
./radare2 -qq -AA <poc_file>
```

Impact
latest commit and latest release

```
$ ./radare2 -v
radare2 5.6.5 27830 @ linux-x86-64 git.5.6.2
commit: 245babbf9e0d45574ee24f1b77b6ca28379dcb14 build: 2022-03-18__07:41:5
$ cat /etc/issue
Ubuntu 20.04.3 LTS \n \l
```

## References

- tests_65185.zip

CVE
CVE-2022-1031
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by
peacock-doris
@peacock-doris
unranked

Fixed by

pancake
@trufae
maintainer

This report was seen 600 times.

We are processing your report and will contact the **radareorg/radare2** team within 24 hours.
8 months ago

We have contacted a member of the **radareorg/radare2** team and are waiting to hear back
8 months ago

**pancake** validated this vulnerability 8 months ago

**peacock-doris** has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

**pancake** marked this as fixed in **5.6.6** with commit **a7ce29** 8 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

pancake 8 months ago Maintainer

The actual bug was fixed in two commits, i just pointed out the last one, but as explained in github, the proper way to fix that is making RRegItem refcounted, which will break abi and probably introduce some memleaks untli properly integrated.

I have pushed the binary in the fuzzed testsuite to ensure that bug doesnt comes back when this refactoring is done.

Thank you!

Sign in to join this conversation