huntr

heap-use-after-free in radareorg/radare2

1

Valid Reported on Apr 5th 2022

Description

Whilst experimenting with `radare2` , built from version 5.6.6, we are able to induce a vulnerability at `reg.c:101` in function `r_reg_get_name_idx` , using `radare2` as a harness.

```
 99:  R_API int r_reg_get_name_idx(const char *type) {
100:    r_return_val_if_fail (type, -1);
//use-after-free here
101:    if (type[0] && type[1] && !type[2])
102:    switch (*type | (type[1] << 8)) {
103:    /* flags */
104:    case 'Z' + ('F' << 8): return R_REG_NAME_ZF;
105:    case 'S' + ('F' << 8): return R_REG_NAME_SF;
106:    case 'C' + ('F' << 8): return R_REG_NAME_CF;
107:    case 'O' + ('F' << 8): return R_REG_NAME_OF;
108:    /* gpr */
109:    case 'P' + ('C' << 8): return R_REG_NAME_PC;
110:    case 'S' + ('R' << 8): return R_REG_NAME_SR;
111:    case 'L' + ('R' << 8): return R_REG_NAME_LR;
112:    case 'S' + ('P' << 8): return R_REG_NAME_SP;
113:    case 'B' + ('P' << 8): return R_REG_NAME_BP;
114:    case 'S' + ('N' << 8): return R_REG_NAME_SN;
115:    /* args */
116:    case 'A' + ('0' << 8): return R_REG_NAME_A0;
117:    case 'A' + ('1' << 8): return R_REG_NAME_A1;
118:    case 'A' + ('2' << 8): return R_REG_NAME_A2;
119:    case 'A' + ('3' << 8): return R_REG_NAME_A3;
120:    case 'A' + ('4' << 8): return R_REG_NAME_A4;
121:    case 'A' + ('5' << 8): return R_REG_NAME_A5;
122:    case 'A' + ('6' << 8): return R_REG_NAME_A6;
123:    case 'A' + ('7' << 8): return R_REG_NAME_A7;
124:    case 'A' + ('8' << 8): return R_REG_NAME_A8;
```

```
  case 'A' + ('8' << 8): return R_REG_NAME_A8;
  case 'A' + ('9' << 8): return R_REG_NAME_A9;
  /* return values */

  case 'R' + ('0' << 8): return R_REG_NAME_R0;
  case 'R' + ('1' << 8): return R_REG_NAME_R1;
  case 'R' + ('2' << 8): return R_REG_NAME_R2;
  case 'R' + ('3' << 8): return R_REG_NAME_R3;
  case 'F' + ('0' << 8): return R_REG_NAME_F0;
  case 'F' + ('1' << 8): return R_REG_NAME_F1;
  case 'F' + ('2' << 8): return R_REG_NAME_F2;
  case 'F' + ('3' << 8): return R_REG_NAME_F3;
  }
  return -1;
}
```

Due to not properly handling pointers, a heap-based use-after-free will be triggered when the software encounters a malformed file, which could result in denial of service.
We found that the vulnerability exists in the latest master branch as well.

Environment

Ubuntu 20.04 LTS x86_64
gcc 10.3.0

Proof of Concept

The POC is: poc
The reproducing process is:

```
# build with address sanitizer
SANITIZE=address ./sys/sanitize.sh
# disable some features of address sanitizer to avoid false positives
export ASAN_OPTIONS=detect_leaks=0:abort_on_error=1:symbolize=1:allocator_m
# trigger the crash
./radare2 -AA -qq POC_FILE
```

The ASAN report is:

```
==92948==ERROR: AddressSanitizer: heap-use-after-free on address 0x60200031
READ of size 1 at 0x60200031b590 thread T0
    #0 0x7ffff1d1e8f5 in r_reg_get_name_idx /work/libraries/radare2-5.6.6/l

    #1 0x7ffff1d204f9 in r_reg_get /work/libraries/radare2-5.6.6/libr/reg/r
    #2 0x7ffff1d203a4 in r_reg_getv /work/libraries/radare2-5.6.6/libr/reg/
    #3 0x7ffff4736f70 in r_core_anal_esil /work/libraries/radare2-5.6.6/lib
    #4 0x7ffff4581bea in cmd_anal_all /work/libraries/radare2-5.6.6/libr/co
    #5 0x7ffff45874d8 in cmd_anal /work/libraries/radare2-5.6.6/libr/core/c
    #6 0x7ffff47024c3 in r_cmd_call /work/libraries/radare2-5.6.6/libr/core
    #7 0x7ffff4638043 in r_core_cmd_subst_i /work/libraries/radare2-5.6.6/l
    #8 0x7ffff462f347 in r_core_cmd_subst /work/libraries/radare2-5.6.6/lib
    #9 0x7ffff463e901 in run_cmd_depth /work/libraries/radare2-5.6.6/libr/c
    #10 0x7ffff463f15d in r_core_cmd /work/libraries/radare2-5.6.6/libr/cor
    #11 0x7ffff463fd0b in r_core_cmd0 /work/libraries/radare2-5.6.6/libr/co
    #12 0x7ffff458090f in cmd_anal_all /work/libraries/radare2-5.6.6/libr/c
    #13 0x7ffff45874d8 in cmd_anal /work/libraries/radare2-5.6.6/libr/core/
    #14 0x7ffff47024c3 in r_cmd_call /work/libraries/radare2-5.6.6/libr/cor
    #15 0x7ffff4638043 in r_core_cmd_subst_i /work/libraries/radare2-5.6.6/
    #16 0x7ffff462f347 in r_core_cmd_subst /work/libraries/radare2-5.6.6/li
    #17 0x7ffff463e901 in run_cmd_depth /work/libraries/radare2-5.6.6/libr/
    #18 0x7ffff463f15d in r_core_cmd /work/libraries/radare2-5.6.6/libr/cor
    #19 0x7ffff463fd0b in r_core_cmd0 /work/libraries/radare2-5.6.6/libr/co
    #20 0x7ffff7185010 in r_main_radare2 /work/libraries/radare2-5.6.6/libr
    #21 0x5555555556ff in main /work/libraries/radare2-5.6.6/binr/radare2/r
    #22 0x7ffff6f6b0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #23 0x55555555528d in _start (/work/libraries/radare2-5.6.6/binr/radare

0x60200031b590 is located 0 bytes inside of 4-byte region [0x60200031b590,0
freed by thread T0 here:
    #0 0x7ffff769b8f7 in __interceptor_free ../../../../src/libsanitizer/as
    #1 0x7ffff1d1f125 in r_reg_free_internal /work/libraries/radare2-5.6.6/
    #2 0x7ffff1d2bd9f in r_reg_set_profile_string /work/libraries/radare2-5
    #3 0x7ffff2b9ffd5 in r_anal_set_reg_profile /work/libraries/radare2-5.6
    #4 0x7ffff2ba04d7 in r_anal_set_bits /work/libraries/radare2-5.6.6/libr
    #5 0x7ffff464fe19 in cb_asmbits /work/libraries/radare2-5.6.6/libr/core
    #6 0x7ffff6da6bce in r_config_set_i /work/libraries/radare2-5.6.6/libr/
    #7 0x7ffff4693017 in r_core_seek_arch_bits /work/libraries/radare2-5.6.
    #8 0x7ffff4736884 in r_core_anal_esil /work/libraries/radare2-5.6.6/lib
    #9 0x7ffff4581bea in cmd_anal_all /work/libraries/radar
    #10 0x7ffff45874d8 in cmd_anal /work/libraries/radare2-5.6.6/libr/core/
    #11 0x7ffff47024c3 in r_cmd_call /work/libraries/radare2-5.6.6/libr/c
    #11 0x7ffff47024c3 in r_cmd_call /work/libraries/radare2-5.6.6/libr/cor
    #12 0x7ffff4638043 in r_core_cmd_subst_i /work/libraries/radare2-5.6.6/
    #13 0x7ffff462f347 in r_core_cmd_subst /work/libraries/radare2-5.6.6/li

    #14 0x7ffff463e901 in run_cmd_depth /work/libraries/radare2-5.6.6/libr/
    #15 0x7ffff463f15d in r_core_cmd /work/libraries/radare2-5.6.6/libr/cor
    #16 0x7ffff463fd0b in r_core_cmd0 /work/libraries/radare2-5.6.6/libr/co
    #17 0x7ffff458090f in cmd_anal_all /work/libraries/radare2-5.6.6/libr/c
    #18 0x7ffff45874d8 in cmd_anal /work/libraries/radare2-5.6.6/libr/core/
    #19 0x7ffff47024c3 in r_cmd_call /work/libraries/radare2-5.6.6/libr/cor
    #20 0x7ffff4638043 in r_core_cmd_subst_i /work/libraries/radare2-5.6.6/
    #21 0x7ffff462f347 in r_core_cmd_subst /work/libraries/radare2-5.6.6/li
    #22 0x7ffff463e901 in run_cmd_depth /work/libraries/radare2-5.6.6/libr/
    #23 0x7ffff463f15d in r_core_cmd /work/libraries/radare2-5.6.6/libr/cor
    #24 0x7ffff463fd0b in r_core_cmd0 /work/libraries/radare2-5.6.6/libr/co
    #25 0x7ffff7185010 in r_main_radare2 /work/libraries/radare2-5.6.6/libr
    #26 0x5555555556ff in main /work/libraries/radare2-5.6.6/binr/radare2/r
    #27 0x7ffff6f6b0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.

previously allocated by thread T0 here:
    #0 0x7ffff76429f7 in __interceptor_strdup ../../../../src/libsanitizer/
    #1 0x7ffff72b2ed8 in r_str_new /work/libraries/radare2-5.6.6/libr/util/
    #2 0x7ffff72b3e62 in r_str_dup /work/libraries/radare2-5.6.6/libr/util/
    #3 0x7ffff1d1ede8 in r_reg_set_name /work/libraries/radare2-5.6.6/libr/
    #4 0x7ffff1d2ab6c in parse_alias /work/libraries/radare2-5.6.6/libr/reg
    #5 0x7ffff1d2c556 in r_reg_set_profile_string /work/libraries/radare2-5
    #6 0x7ffff2b9ffd5 in r_anal_set_reg_profile /work/libraries/radare2-5.6
    #7 0x7ffff2ba04d7 in r_anal_set_bits /work/libraries/radare2-5.6.6/libr
    #8 0x7ffff464fe19 in cb_asmbits /work/libraries/radare2-5.6.6/libr/core
    #9 0x7ffff6da6bce in r_config_set_i /work/libraries/radare2-5.6.6/libr/
    #10 0x7ffff4693017 in r_core_seek_arch_bits /work/libraries/radare2-5.6
    #11 0x7ffff4736884 in r_core_anal_esil /work/libraries/radare2-5.6.6/li
    #12 0x7ffff4581bea in cmd_anal_all /work/libraries/radare2-5.6.6/libr/c
    #13 0x7ffff45874d8 in cmd_anal /work/libraries/radare2-5.6.6/libr/core/
    #14 0x7ffff47024c3 in r_cmd_call /work/libraries/radare2-5.6.6/libr/cor
    #15 0x7ffff4638043 in r_core_cmd_subst_i /work/libraries/radare2-5.6.6/
    #16 0x7ffff462f347 in r_core_cmd_subst /work/libraries/radare2-5.6.6/li
    #17 0x7ffff463e901 in run_cmd_depth /work/libraries/radare2-5.6.6/libr/
    #18 0x7ffff463f15d in r_core_cmd /work/libraries/radare2
    #19 0x7ffff463fd0b in r_core_cmd0 /work/libraries/radar
    #20 0x7ffff458090f in cmd_anal_all /work/libraries/radare2-5.6.6/libr/c
    #21 0x7ffff45874d8 in cmd_anal /work/libraries/radare2-5.6.6/libr/core/
    #22 0x7ffff47024c3 in r_cmd_call /work/libraries/radare2-5.6.6/libr/cor
    #23 0x7ffff4638043 in r_core_cmd_subst_i /work/libraries/radare2-5.6.6/

    #24 0x7ffff462f347 in r_core_cmd_subst /work/libraries/radare2-5.6.6/li
    #25 0x7ffff463e901 in run_cmd_depth /work/libraries/radare2-5.6.6/libr/
    #26 0x7ffff463f15d in r_core_cmd /work/libraries/radare2-5.6.6/libr/cor
    #27 0x7ffff463fd0b in r_core_cmd0 /work/libraries/radare2-5.6.6/libr/co
    #28 0x7ffff7185010 in r_main_radare2 /work/libraries/radare2-5.6.6/libr
    #29 0x5555555556ff in main /work/libraries/radare2-5.6.6/binr/radare2/r

SUMMARY: AddressSanitizer: heap-use-after-free /work/libraries/radare2-5.6.
Shadow bytes around the buggy address:
  0x0c048005b660: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c048005b670: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c048005b680: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c048005b690: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c048005b6a0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
=>0x0c048005b6b0: fa fa[fd]fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c048005b6c0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c048005b6d0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c048005b6e0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c048005b6f0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c048005b700: fa fa fd fa fa fa fd fa fa fa fd fa fa fa 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

  ==92948==ABORTING
  Aborted
```

Impact

This vulnerability is capable of inducing denial of service.

CVE
CVE-2022-1284
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.5)

Registry
Other

Affected Version
5.6.6

Visibility
Public

Status
Fixed

Found by

hdthky
@hdthky
unranked

Fixed by

pancake
@trufae
maintainer

This report was seen 651 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 8 months ago Maintainer

I can reproduce! working on the fix right now

pancake 8 months ago Maintainer

Good catch! thank you for reporting! this is causing a random DoS

pancake validated this vulnerability 8 months ago

hdthky has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

pancake marked this as fixed in **5.6.8** with commit **64a82e** 8 months ago

pancake has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

hdthky 7 months ago Researcher

This bug was found by Xingyuan Mo from 360 IceSword Lab

Sign in to join this conversation

Chat with us