Use After Free in r_reg_get_name_idx in radareorg/radare2

0

Valid Reported on Mar 3rd 2022

Description

heap use after free in r_reg_get_name_idx.
ASAN report:

```
=================================================================
==1710816==ERROR: AddressSanitizer: heap-use-after-free on address 0x602000
READ of size 1 at 0x6020001dff50 thread T0
    #0 0x7fa7c085d87b in r_reg_get_name_idx /root/radare2-5.6.4/libr/reg/re
    #1 0x7fa7c08610c7 in r_reg_get /root/radare2-5.6.4/libr/reg/reg.c:321
    #2 0x7fa7c0860ed1 in r_reg_setv /root/radare2-5.6.4/libr/reg/reg.c:301
    #3 0x7fa7cb191d52 in r_core_anal_esil /root/radare2-5.6.4/libr/core/car
    #4 0x7fa7cae699b0 in cmd_anal_all /root/radare2-5.6.4/libr/core/cmd_ana
    #5 0x7fa7cae72d1d in cmd_anal /root/radare2-5.6.4/libr/core/cmd_anal.c:
    #6 0x7fa7cb1321d7 in r_cmd_call /root/radare2-5.6.4/libr/core/cmd_api.c
    #7 0x7fa7cafb1f28 in r_core_cmd_subst_i /root/radare2-5.6.4/libr/core/c
    #8 0x7fa7cafa1e07 in r_core_cmd_subst /root/radare2-5.6.4/libr/core/cmc
    #9 0x7fa7cafbe764 in run_cmd_depth /root/radare2-5.6.4/libr/core/cmd.c:
    #10 0x7fa7cafbf7db in r_core_cmd /root/radare2-5.6.4/libr/core/cmd.c:54
    #11 0x7fa7cafc07d4 in r_core_cmd0 /root/radare2-5.6.4/libr/core/cmd.c:5
    #12 0x7fa7cae67039 in cmd_anal_all /root/radare2-5.6.4/libr/core/cmd_ar
    #13 0x7fa7cae72d1d in cmd_anal /root/radare2-5.6.4/libr/core/cmd_anal.c
    #14 0x7fa7cb1321d7 in r_cmd_call /root/radare2-5.6.4/libr/core/cmd_api.
    #15 0x7fa7cafb1f28 in r_core_cmd_subst_i /root/radare2-5.6.4/libr/core/
    #16 0x7fa7cafa1e07 in r_core_cmd_subst /root/radare2-5.6.4/libr/core/cm
    #17 0x7fa7cafbe764 in run_cmd_depth /root/radare2-5.6.4/libr/core/cmd.c
    #18 0x7fa7cafbf7db in r_core_cmd /root/radare2-5.6.4/libr/core/cmd.c:54
    #19 0x7fa7cafc07d4 in r_core_cmd0 /root/radare2-5.6.4/libr/core/cmd.c:5
    #20 0x7fa7d36ee1cd in r_main_radare2 /root/radare2-5.6.4/libr/main/rad
    #21 0x557bc4deb937 in main /root/radare2/binr/radare2/r
    #22 0x7fa7d2aee0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #23 0x557bc4deb30d in _start (/root/radare2/binr/radare2/radare2+0x230d
```

```
#23 0x557bc4deb30d in _start (/root/radare2/binr/radare2/radare2+0x230d
```

How can we reproduce the issue?

Compile command

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

reproduce command
poc_uaf_r_reg_get.zip

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

Impact

latest commit and latest release

```
$ ./radare2 -v
radare2 5.6.4 27751 @ linux-x86-64 git.5.6.2
commit: d1b1d52f695d287667690d130ad2569aed8aa2ff build: 2022-03-03__07:18:1
$ cat /etc/issue
Ubuntu 20.04.3 LTS \n \l
```

References

- poc_uaf_r_reg_get.zip

CVE
CVE-2022-0849
(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 552 times.

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

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

pancake validated this vulnerability 9 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 **10517e** 9 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘