huntr

Out-of-bounds Read in radareorg/radare2

0

✓ Valid Reported on Dec 30th 2021

Description

This vulnerability is of out-of-bound read. The bug exists in latest stable release (radare2-5.5.4). Specifically, the vulnerable code is picked out as follows:

```
//  libr/util/buf.c line 631
R_API void r_buf_fini(RBuffer *b) {
...
// the pointer address of b->methods is broken
if (b->methods->get_whole_buf) {
...
```

Proof of Concept

Build the radare2 5.5.4, download the POC_FILE. Then run

```
# trigger the crash
radare2 -A -q POC_FILE
```

The crash stack information is:

```
#0  0x00007ffff7e33e7d in r_buf_fini (b=0x5555558f2d20)
    at buf.c:631
#1  r_buf_free (b=0x5555558f2d20) at buf.c:643
#2  0x00007ffff6224872 in r_bin_file_free (_bf=0x5555558f2680)
    at bfile.c:733
#3  0x00007ffff7e3af29 in r_list_delete (list=0x5555558068e0,
    iter=0x5555558f2900) at list.c:123
#4  r_list_purge (list=0x5555558068e0) at list.c:89
#5  r_list_free (list=0x5555558068e0) at list.c:99
```

```
#6  0x00007ffff6210d12 in r_bin_free (bin=0x5555558072a0)
    at bin.c:469
#7  0x00007ffff6563a86 in r_core_fini (c=0x555555761ce0)

    at core.c:3096
#8  0x00007ffff6563bef in r_core_free (c=c@entry=0x555555761ce0)
    at core.c:3123
#9  0x00007ffff7da1ac5 in r_main_radare2 (argc=4,
    argv=<optimized out>) at radare2.c:1554
#10 0x00007ffff7bb20b3 in __libc_start_main ()
   from /lib/x86_64-linux-gnu/libc.so.6
#11 0x00005555555562ae in _start ()
```

Impact

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) if the broken pointer address (b->methods) can be further exploited (need more investigation).

References

- poc file

CVE
CVE-2022-0173
(Published)

Vulnerability Type
CWE-125: Out-of-bounds Read

Severity
Critical (9.6)

Visibility
Public

Status
Fixed

Found by

Cen Zhang
@occia
unranked

Chat with us

This report was seen 416 times.

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

Cen Zhang modified the report a year ago

Cen Zhang modified the report a year ago

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

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

A **radareorg/radare2** maintainer validated this vulnerability a year ago

Cen Zhang has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **radareorg/radare2** maintainer marked this as fixed in **Will be fixed in the upcoming r2-5.6.0** with commit **378972** a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Cen Zhang 10 months ago Researcher

Hi, you might link the patch of the use-after-free to this oob bug by mistake. And I've tested the radare2 with latest commit (ed2030b79e68986bf04f3a6279463ab989fe400f), the bug is still at there.

I don't know how to completely fix this bug, however, I think the fix should be locating the code where breaks the address of `b->methods` since the POC shows that it is already a wild pointer when program executes to L631.

Cen Zhang 10 months ago

Chat with us

Sorry, I messed up the radare2 binaries in my environment, the bug has been fixed in latest

Sorry, I messed up the radare2 binaries in my environment, the bug has been fixed in latest commit~ Sorry for the caused inconvenience!

Sign in to join this conversation