huntr

Out-of-bounds read in `r_bin_ne_get_relocs` function in radareorg/radare2

0

✓ Valid Reported on Apr 6th 2022

Description

Out-of-bounds (OOB) read vulnerability exists in `r_bin_ne_get_relocs` function in Radare2 5.6.7 due to a missing check on the index value.

Version

```
radare2 5.6.7 27746 @ linux-x86-64 git.5.6.6
commit: 2b77b277d67ce061ee6ef839e7139ebc2103c1e3 build: 2022-04-06__14:41:3
```

Proof of Concept

```
radare2 -q -A poc
```

poc

Analysis

The buffer is allocated at `/format/ne/ne.c:442`

```
ut16 *modref = calloc (bin->ne_header->ModRefs, sizeof (ut16));
    if (!modref) {
        return NULL;
    }
```

The out-of-boud read happens at `/format/ne/ne.c:517` due to a missing check on `rel.index`

```
            if (rel.index > bin->ne_header->ModRefs) {
                name = r_str_newf ("UnknownModule%d_%x", rel.index, of
            } else {
                offset = modref[rel.index - 1] + bin->header_offset + b
                name = __read_nonnull_str_at (bin->buf, offset);
            }
```

ASAN

```
==2173198==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200
READ of size 2 at 0x60200006938e thread T0
    #0 0x7f394f24f0b0 in r_bin_ne_get_relocs /root/fuzzing/radare2_fuzzing/
    #1 0x7f394f24c9d2 in relocs /root/fuzzing/radare2_fuzzing/radare2/libr/
    #2 0x7f394f0ec251 in r_bin_object_set_items /root/fuzzing/radare2_fuzzi
    #3 0x7f394f0ed565 in r_bin_object_new /root/fuzzing/radare2_fuzzing/rad
    #4 0x7f394f0e6fe1 in r_bin_file_new_from_buffer /root/fuzzing/radare2_f
    #5 0x7f394f0ca8ca in r_bin_open_buf /root/fuzzing/radare2_fuzzing/radar
    #6 0x7f394f0cb1ff in r_bin_open_io /root/fuzzing/radare2_fuzzing/radare
    #7 0x7f394f8b35d9 in r_core_file_do_load_for_io_plugin /root/fuzzing/ra
    #8 0x7f394f8b35d9 in r_core_bin_load /root/fuzzing/radare2_fuzzing/rada
    #9 0x7f3951c6167f in r_main_radare2 /root/fuzzing/radare2_fuzzing/radar
    #10 0x562b58c2d27e in main /root/fuzzing/radare2_fuzzing/radare2/binr/r
    #11 0x7f3951a717fc in __libc_start_main ../csu/libc-start.c:332
    #12 0x562b58c2d179 in _start (/root/fuzzing/radare2_fuzzing/radare2/bin

0x60200006938e is located 2 bytes to the left of 1-byte region [0x602000069
allocated by thread T0 here:
    #0 0x7f39520bc987 in __interceptor_calloc ../../../../src/libsanitizer/
    #1 0x7f394f24e7c2 in r_bin_ne_get_relocs /root/fuzzing/radare2_fuzzing/

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/fuzzing/radare2_fuzzi
Shadow bytes around the buggy address:
  0x0c0480005220: fa fa 00 07 fa fa 00 fa fa fa 00 06 fa fa 00 07
  0x0c0480005230: fa fa 00 05 fa fa 00 06 fa fa 00 05 fa fa fd fd
  0x0c0480005240: fa fa fd fd fa fa fd fa fa fa fd fd fa fa
  0x0c0480005250: fa fa fd fd fa fa fd fd fa fa fd fd fa fa
  0x0c0480005260: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
```

```
=>0x0c0480005270: fa[fa]01 fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480005280: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480005290: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800052a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800052b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800052c0: fa fa fa fa 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
```

Backtrace

```
#0  r_bin_ne_get_relocs (bin=0x608000020120) at /root/fuzzing/radare2_fuzzi
#1  0x00007ffff3a1cf29 in relocs (bf=0x60d0000006c0) at /root/fuzzing/radar
#2  0x00007ffff36fb3de in r_bin_object_set_items (bf=0x60d0000006c0, bo=0x6
#3  0x00007ffff36f8554 in r_bin_object_new (bf=0x60d0000006c0, plugin=0x613
#4  0x00007ffff36e4e4d in r_bin_file_new_from_buffer (bin=0x616000000c80, f
#5  0x00007ffff36a14bd in r_bin_open_buf (bin=0x616000000c80, buf=0x6030000
#6  0x00007ffff369fec8 in r_bin_open_io (bin=0x616000000c80
#7  0x00007ffff462b676 in r_core_file_do_load_for_io_plugin
#8  0x00007ffff462396a in r_core_bin_load (r=0x7fffee032800, filenameuri=0x
```

Chat with us

```
#9  0x00007ffff77132d3 in r_main_radare2 (argc=4, argv=0x7fffffffe498) at r
#10 0x000055555561ee50 in main (argc=4, argv=0x7fffffffe498) at radare2.c:9

#11 0x00007ffff74aa7fd in __libc_start_main (main=0x55555561ecf0 <main>, ar
#12 0x00005555555753ba in _start ()
```

Impact

This vulnerability may allow attackers to read sensitive information or cause a crash.

CVE
CVE-2022-1296
(Published)

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

Severity
Medium (6.6)

Registry
Other

Affected Version
5.6.7

Visibility
Public

Status
Fixed

Found by

hmthabit
@hmthabit
unranked

Fixed by

pancake
@trufae
maintainer

Chat with us

This report was seen 579 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 has marked this vulnerability as informative 8 months ago

Can't reproduce on master

The disclosure bounty has been dropped ✗

The fix bounty has been dropped ✗

hmthabit 8 months ago Researcher

Please check if you used the correct POC.

I've tried it agian on the latest commit and it works without any problem

```
radare2 -v
radare2 5.6.7 27748 @ linux-x86-64 git.5.6.6
commit: 18d1d064bf599a255d55f09fca3104776fc34a67 build: 2022-04-08__14:04:24
```

pancake 8 months ago Maintainer

You are right, i tested it wrongly. i have fixed it but i see no way to reopen this ticket. maybe we should call support? https://github.com/radareorg/radare2/pull/19923

Sorry for that and thanks for reporting it! nice catch!

Chat with us

hmthabit 8 months ago Researcher

Thanks for responding

@admin can you please reclassify this issue?

pancake 8 months ago Maintainer

Can you confirm now?

hmthabit 8 months ago Researcher

It's fixed now. Thanks

Jamie Slome 8 months ago Admin

Sorted 🎉

@maintainer - feel free to use the dropdown below to close the report accordingly and to mark the report as fixed 👍

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

pancake validated this vulnerability 8 months ago

hmthabit 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 **153bcd** 8 months ago

pancake has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us