Out-of-bounds read in radareorg/radare2

0

✓ Valid Reported on Apr 1st 2022

Description

Out-of-bounds (OOB) read vulnerability exists in analop function in Radare2 5.6.7

Version

```
radare2 5.6.7 27722 @ linux-x86-64 git.5.6.6
commit: e876eef2a2f758157dd6028fb01809bcedacf00f build: 2022-04-01__07:03:3
```

Proof of Concept

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

poc

ASAN

```
==2143069==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200
READ of size 1 at 0x6020000a2a17 thread T0
    #0 0x7fabd14c6e66 in analop /root/fuzzing/radare2_fuzzing/radare2/libr/
    #1 0x7fabd15ee0b7 in r_anal_op /root/fuzzing/radare2_fuzzing/radare2/li
    #2 0x7fabd2edd954 in anal_block_cb /root/fuzzing/radare2_fuzzing/radare
    #3 0x7fabd1618bab in r_anal_block_recurse_depth_first /root/fuzzing/rac
    #4 0x7fabd2ede480 in r_core_recover_vars /root/fuzzing/radare2_fuzzing/
    #5 0x7fabd2cf8d40 in r_core_af /root/fuzzing/radare2_fuzzing/radare2/li
    #6 0x7fabd2ee2f29 in r_core_anal_all /root/fuzzing/rada
    #7 0x7fabd2d33ac1 in cmd_anal_all /root/fuzzing/radare2_
    #8 0x7fabd2d3bc5b in cmd_anal /root/fuzzing/radare2_fuzzing/radare2/lib
```

Chat with us

```
    #9 0x7fabd2eb7d8a in r_cmd_call /root/fuzzing/radare2_fuzzing/radare2/l
    #10 0x7fabd2dece8c in r_core_cmd_subst_i /root/fuzzing/radare2_fuzzing/
    #11 0x7fabd2de4103 in r_core_cmd_subst /root/fuzzing/radare2_fuzzing/ra
    #12 0x7fabd2df3792 in run_cmd_depth /root/fuzzing/radare2_fuzzing/radar
    #13 0x7fabd2df4002 in r_core_cmd /root/fuzzing/radare2_fuzzing/radare2/
    #14 0x7fabd2df4b2c in r_core_cmd0 /root/fuzzing/radare2_fuzzing/radare2
    #15 0x7fabd54f93ca in r_main_radare2 /root/fuzzing/radare2_fuzzing/rada
    #16 0x5652f8dde5f8 in main /root/fuzzing/radare2_fuzzing/radare2/binr/r
    #17 0x7fabd52f97fc in __libc_start_main ../csu/libc-start.c:332
    #18 0x5652f8dde179 in _start (/root/fuzzing/radare2_fuzzing/radare2/bir

0x6020000a2a17 is located 0 bytes to the right of 7-byte region [0x6020000a
allocated by thread T0 here:
    #0 0x7fabd59fe7cf in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x7fabd2edd2ef in anal_block_cb /root/fuzzing/radare2_fuzzing/radare
    #2 0x7fabd1618bab in r_anal_block_recurse_depth_first /root/fuzzing/rad
    #3 0x7fabd2ede480 in r_core_recover_vars /root/fuzzing/radare2_fuzzing/
    #4 0x7fabd2cf8d40 in r_core_af /root/fuzzing/radare2_fuzzing/radare2/li
    #5 0x7fabd2ee2f29 in r_core_anal_all /root/fuzzing/radare2_fuzzing/rada
    #6 0x7fabd2d33ac1 in cmd_anal_all /root/fuzzing/radare2_fuzzing/radare2
    #7 0x7fabd2d3bc5b in cmd_anal /root/fuzzing/radare2_fuzzing/radare2/lib
    #8 0x7fabd2eb7d8a in r_cmd_call /root/fuzzing/radare2_fuzzing/radare2/l
    #9 0x7fabd2dece8c in r_core_cmd_subst_i /root/fuzzing/radare2_fuzzing/r
    #10 0x7fabd2de4103 in r_core_cmd_subst /root/fuzzing/radare2_fuzzing/ra
    #11 0x7fabd2df3792 in run_cmd_depth /root/fuzzing/radare2_fuzzing/radar
    #12 0x7fabd2df4002 in r_core_cmd /root/fuzzing/radare2_fuzzing/radare2/
    #13 0x7fabd2df4b2c in r_core_cmd0 /root/fuzzing/radare2_fuzzing/radare2
    #14 0x7fabd54f93ca in r_main_radare2 /root/fuzzing/radare2_fuzzing/rada
    #15 0x5652f8dde5f8 in main /root/fuzzing/radare2_fuzzing/radare2/binr/r
    #16 0x7fabd52f97fc in __libc_start_main ../csu/libc-start.c:332

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/fuzzing/radare2_fuzzi
Shadow bytes around the buggy address:
  0x0c048000c4f0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c048000c500: fa fa fd fa fa fa fd fa fa fa 06 fa fa fa fd fa
  0x0c048000c510: fa fa fd fa fa fa fd fa fa fa fd fd fa fa 00 05
  0x0c048000c520: fa fa 00 fa fa fa 00 02 fa fa fd fd fa fa 00 05
  0x0c048000c530: fa fa 00 05 fa fa 00 05 fa fa fd fd fa fa
=>0x0c048000c540: fa fa[07]fa fa fa 04 fa fa fa 03 fa fa fa
  0x0c048000c550: fa fa 03 fa fa fa 03 fa fa fa fa fa fa fa fa fa
  0x0c048000c560: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c048000c570: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c048000c580: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

  0x0c048000c590: 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
==2143069==ABORTING
```

Backtrace

```
#7  0x00007ffff3149e67 in analop (a=0x61a000000680, op=0x7fffffffd170, addr
#8  0x00007ffff32710b8 in r_anal_op (anal=0x61a000000680, op=0x7fffffffd17
#9  0x00007ffff4b60955 in anal_block_cb (bb=0x611000014e00, ctx=0x7fffffffc
#10 0x00007ffff329bbac in r_anal_block_recurse_depth_first (block=0x611000
#11 0x00007ffff4b61481 in r_core_recover_vars (core=0x7fffef60f800, fcn=0x6
#12 0x00007ffff497bd41 in r_core_af (core=0x7fffef60f800, addr=65536, name=
#13 0x00007ffff4b65f2a in r_core_anal_all (core=0x7fffef60f800) at canal.c:
#14 0x00007ffff49b6ac2 in cmd_anal_all (core=0x7fffef60f800
#15 0x00007ffff49bec5c in cmd_anal (data=0x7fffef60f800, inp
#16 0x00007ffff4b3ad8b in r_cmd_call (cmd=0x620000000080, input=0x6020000a2
#17 0x00007ffff4a6fe8d in r_core_cmd_subst_i (core=0x7fffef60f800, cmd=0x66
#18 0x00007ffff4a67104 in r_core_cmd_subst (core=0x7fffef60f800, cmd=0x602
#19 0x00007ffff4a76793 in run_cmd_depth (core=0x7fffef60f800, cmd=0x621000
#20 0x00007ffff4a77003 in r_core_cmd (core=0x7fffef60f800, cstr=0x7ffff719
#21 0x00007ffff4a77b2d in r_core_cmd0 (core=0x7fffef60f800, cmd=0x7ffff719
#22 0x00007ffff717c3cb in r_main_radare2 (argc=4, argv=0x7fffffffe468) at r
#23 0x00005555555555f9 in main (argc=4, argv=0x7fffffffe468) at radare2.c:9
#24 0x00007ffff6f7c7fd in __libc_start_main (main=0x555555555581 <main>, ar
#25 0x000055555555517a in _start ()
```

Analysis

The buffer is allocated at `/libr/core/canal.c:3452` with `bb->size`

```
static bool anal_block_cb(RAnalBlock *bb, BlockRecurseCtx *ctx) {
    if (r_cons_is_breaked ()) {
        return false;
    }
    if (bb->size < 1) {
        return true;
    }
    if (bb->size > ctx->core->anal->opt.bb_max_size) {
        return true;
    }
    ut8 *buf = malloc (bb->size);
    if (!buf) {
        return false;
    }
    (void) r_io_read_at (ctx->core->io, bb->addr, buf, bb->size);
```

Then at `/libr/core/canal.c:3502` , `pos` value is added to the pointer `buf` before being passed to `r_anal_op` function

```
#else
        pos = (opaddr - bb->addr);
        if (r_anal_op (core->anal, &op, opaddr, buf + pos,
            break;
        }
```

`r_anal_op` function passes the arguments to `op` function without any validiation on `data`

```
ret = anal->cur->op (anal, op, addr, data, len, mask);
```

The OOB read happens at `/libr/anal/p/anal_cris.c:65` when it tries to read `buf[1]`

```
static int analop(RAnal *a, RAnalOp *op, ut64 addr, const ut8 *buf, int len
    default:
        switch (buf[1]) {                  // <<<<< OOB read
        case 0x00:
            op->type = R_ANAL_OP_TYPE_CJMP; // BCC
            break;
```

Suggested Fix

Validate `buf` size after adding `pos` at `/libr/core/canal.c:3502`

Impact

This vulnerability allows attackers to read sensitive information from outside the allocated buffer boundary.

CVE
CVE-2022-1207
(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

This report was seen 638 times.

We are processing your report and will contact the **radareorg/radare2** team within 24 hours. 8 months ago

hmthabit modified the report 8 months ago

hmthabit modified the report 8 months ago

hmthabit modified the report 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 **605785** 8 months ago

pancake has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

> Sign in to join this conversation