huntr

Improper Validation of Array Index in radareorg/radare2

0

✓ Valid Reported on Apr 4th 2022

This vulnerability is of type Improper Validation of Array Index. The bug exists in latest stable release (radare2-5.6.6) and lastest master branch (8317a34b7e4ab731e230dcdd81adc9323c5b518b, updated in April 03, 2022). Specifically, the vulnerable code (located at `libr/bin/format/ne/ne.c`) and the bug's basic explanation are highlighted as follows:

```
                        RBinSection *bs = R_NEW0 (RBinSection);
// i is not well validated.
                        NE_image_segment_entry *se = &bin->segment_entries[
                        if (!bs) {
                                return segments;
                        }
// seed1 can trigger this heap overflow.
                        bs->size = se->length;
                        bs->vsize = se->minAllocSz ? se->minAllocSz : 6400
                        bs->bits = R_SYS_BITS_16;
                        bs->is_data = se->flags & IS_DATA;
                        bs->perm = __translate_perms (se->flags);
```

```
                                        char *name;
                                        if (rel.index > bin->ne_header->Mo
                                                name = r_str_newf ("Unknow
                                        } else {
                                                printf("modref addr: %X, bi
// Seed2 can trigger this heap overflow. The rel.index is not validated an
                                                offset = modref[rel.index -
                                                name = __read_nonnull_str_a
                                        }
                                        if (rel.flags & IMPORTED_ORD) {
                                                imp->ordinal = rel.func_ord
```

```
498                                              imp->ordinal = rel.func_ord
```

Proof of Concept

Build the radare2 (8317a34b7e4ab731e230dcdd81adc9323c5b518b, updated in April 03, 2022) 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 crash stack is:

```
# seed1
=================================================================
==28776==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62f000
READ of size 2 at 0x62f00000deda thread T0
    #0 0x7ffff2a83100  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #1 0x7ffff2a84696  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #2 0x7ffff264667f  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #3 0x7ffff2645004  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #4 0x7ffff262a1fe  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #5 0x7ffff25cd9fb  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #6 0x7ffff25ccad6  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #7 0x7ffff384136c  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #8 0x7ffff7548697  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #9 0x7ffff72bc0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #10 0x55555557239d  (/src/cmdline-fuzz/exprs/radare2-5.5.4/radare2+0x1e

0x62f00000deda is located 2 bytes to the right of 56024-byte region [0x62f0
allocated by thread T0 here:
    #0 0x5555555ed772  (/src/cmdline-fuzz/exprs/radare2-5.5
    #1 0x7ffff2a895dd  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #2 0x7ffff2a8b3fb  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #3 0x7ffff262a1fe  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l


SUMMARY: AddressSanitizer: heap-buffer-overflow (/src/cmdline-fuzz/exprs/ra
Shadow bytes around the buggy address:
  0x0c5e7fff9b80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5e7fff9b90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5e7fff9ba0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5e7fff9bb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5e7fff9bc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c5e7fff9bd0: 00 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa fa
  0x0c5e7fff9be0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5e7fff9bf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5e7fff9c00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5e7fff9c10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5e7fff9c20: 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
==28776==ABORTING

Program received signal SIGABRT, Aborted.
0x00007ffff72db18b in raise () from /lib/x86_64-linux-gnu/libc.so.6
```

```
(gdb) bt
#0  0x00007ffff72db18b in raise () from /lib/x86_64-linux-gnu/libc.so.6

#1  0x00007ffff72ba859 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  0x00005555555f3828 in __asan_report_load2 ()
#7  0x00007ffff2a83101 in r_bin_ne_get_segments (bin=<optimized out>) at /s
#8  0x00007ffff2a84697 in r_bin_ne_get_entrypoints (bin=<optimized out>) at
#9  0x00007ffff2646680 in r_bin_object_set_items (bf=<optimized out>, bo=<o
#10 0x00007ffff2645005 in r_bin_object_new (bf=<optimized out>, plugin=<opt
#11 0x00007ffff262a1ff in r_bin_file_new_from_buffer (bin=0x616000000680, f
    pluginname=<optimized out>) at bfile.c:585
#12 0x00007ffff25cd9fc in r_bin_open_buf (bin=<optimized out>, buf=<optimiz
#13 0x00007ffff25ccad7 in r_bin_open_io (bin=0x616000000680, opt=<optimized
#14 0x00007ffff384136d in r_core_file_do_load_for_io_plugin (r=0x7fffec2d38
#15 r_core_bin_load (r=0x7fffec2d3800, filenameuri=<optimized out>, baddr=<
#16 0x00007ffff7548698 in r_main_radare2 (argc=<optimized out>, argv=<optim
#17 0x00007ffff72bc0b3 in __libc_start_main () from /lib/x86_64-linux-gnu/l
#18 0x000055555557239e in _start ()
```

```
# seed2
=================================================================
==28700==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000
READ of size 2 at 0x60200006c50e thread T0
    #0 0x7ffff2a88d18  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #1 0x7ffff26477f9  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #2 0x7ffff2645004  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #3 0x7ffff262a1fe  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #4 0x7ffff25cd9fb  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #5 0x7ffff25ccad6  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #6 0x7ffff384136c  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #7 0x7ffff7548697  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #8 0x7ffff72bc0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x2
    #9 0x55555557239d  (/src/cmdline-fuzz/exprs/radare2-5.5
```

Chat with us

```
0x60200006c50e is located 2 bytes to the left of 1-byte region [0x60200006
allocated by thread T0 here:
    #0 0x5555555ed5fd  (/src/cmdline-fuzz/exprs/radare2-5.5.4/radare2+0x99

    #1 0x7ffff2a86194  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/
    #2 0x7ffff26477f9  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/src/cmdline-fuzz/exprs/ra
Shadow bytes around the buggy address:
  0x0c0480005850: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c0480005860: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c0480005870: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c0480005880: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c0480005890: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
=>0x0c04800058a0: fa[fa]01 fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800058b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800058c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800058d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800058e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800058f0: 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
==28700==ABORTING
```

```
Program received signal SIGABRT, Aborted.
0x00007ffff72db18b in raise () from /lib/x86_64-linux-gnu/libc.so.6


(gdb) bt
#0  0x00007ffff72db18b in raise () from /lib/x86_64-linux-gnu/libc.so.6
#1  0x00007ffff72ba859 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  0x00005555555f3828 in __asan_report_load2 ()
#7  0x00007ffff2a88d19 in r_bin_ne_get_relocs (bin=<optimized out>) at /sr
#8  0x00007ffff26477fa in r_bin_object_set_items (bf=<optimized out>, bo=<
#9  0x00007ffff2645005 in r_bin_object_new (bf=<optimized out>, plugin=<opt
#10 0x00007ffff262a1ff in r_bin_file_new_from_buffer (bin=0x616000000680, f
    pluginname=<optimized out>) at bfile.c:585
#11 0x00007ffff25cd9fc in r_bin_open_buf (bin=<optimized out>, buf=<optimiz
#12 0x00007ffff25ccad7 in r_bin_open_io (bin=0x616000000680, opt=<optimize
#13 0x00007ffff384136d in r_core_file_do_load_for_io_plugin (r=0x7fffec2d3
#14 r_core_bin_load (r=0x7fffec2d3800, filenameuri=<optimized out>, baddr=<
#15 0x00007ffff7548698 in r_main_radare2 (argc=<optimized out>, argv=<optim
#16 0x00007ffff72bc0b3 in __libc_start_main () from /lib/x86_64-linux-gnu/l
#17 0x000055555557239e in _start ()
```

Impact

This vulnerability is heap overflow and may be exploitable. For more general description of heap buffer overflow, see CWE.

Occurrences

C ne.c L490

References

- PoC files

CVE
CVE-2022-1237

(Published)

Vulnerability Type
CWE-129: Improper Validation of Array Index

Severity
High (7.6)

Registry
Other

Affected Version
5.6.6

Visibility
Public

Status
Fixed

Found by

HanOnly
@hanOnly
legend

Fixed by

pancake
@trufae
maintainer

This report was seen 617 times.

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

HanOnly modified the report 8 months ago

We have contacted a member of the **radareorg/radare2** team and are waiti
8 months ago

Chat with us

pancake validated this vulnerability 8 months ago

Han0nly 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 **2d782c** 8 months ago

pancake has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

ne.c#L490 has been validated ✓

pancake 8 months ago

sorry for the late reply, the huntr dev ui changed and i couldnt find the "fix button"

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

part of 418sec

company

about

team

Chat with us