Heap-based Buffer Overflow in libr/bin/format/ne/ne.c in radareorg/radare2

0

Valid Reported on Apr 4th 2022

This vulnerability is of type heap-buffer-overflow. And after quick investigation I think it is very likely to be successfully exploited to remote code execution. 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:

```
while (off < bin->ne_header->EntryTableLength) {
        ut8 bundle_length = *(ut8 *)(bin->entry_table + off);
        if (!bundle_length) {
            break;
        }
        off++;
// line 382: sample1 can trigger this heap overflow. This may due to the of
        ut8 bundle_type = *(ut8 *)(bin->entry_table + off);
        off++;
        int i;
        for (i = 0; i < bundle_length; i++) {
            entry = R_NEW0 (RBinAddr);
            if (!entry) {
                r_list_free (entries);
                return NULL;
            }
            off++;
            if (!bundle_type) { // Skip
                off--;
                free (entry);
                break;
            } else if (bundle_type == 0xFF) { // Moveable
                off += 2;
                ut8 segnum = *(bin->entry_table + off);
```

```
                ut8 segnum = *(bin->entry_table + off);
                off++;
                ut16 segoff = *(ut16 *)(bin->entry_table + off);
// line 401: sample2 can trigger this heap overflow.
                entry->paddr = (ut64)bin->segment_entries[segnum - 1].offse
            } else { // Fixed
// line 403: sample3 can trigger this heap overflow.
                entry->paddr = (ut64)bin->segment_entries[bundle_type - 1].
            }
            off += 2;
            r_list_append (entries, entry);
        }
    }
```

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:

```
# sample1
=================================================================
==28464==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000(
READ of size 1 at 0x602000065471 thread T0
    #0 0x7ffff2a856ac  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
    #1 0x7ffff264667f  (/src/cmdline-fuzz/exprs/radare2-5.5
    #2 0x7ffff2645004  (/src/cmdline-fuzz/exprs/radare2-5.5
    #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+0x270b2)
    #9 0x55555557239d  (/src/cmdline-fuzz/exprs/radare2-5.5.4/radare2+0x1e3

0x602000065471 is located 0 bytes to the right of 1-byte region [0x6020000(
allocated by thread T0 here:
    #0 0x5555555ed772  (/src/cmdline-fuzz/exprs/radare2-5.5.4/radare2+0x997
    #1 0x7ffff2a89655  (/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:
  0x0c0480004a30: fa fa 04 fa fa fa 03 fa fa fa 04 fa fa fa 04 fa
  0x0c0480004a40: fa fa 04 fa fa fa fd fa fa fa 07 fa fa fa fd fa
  0x0c0480004a50: fa fa 06 fa fa fa fd fa fa fa 06 fa fa fa fd fa
  0x0c0480004a60: fa fa 06 fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480004a70: fa fa fd fa fa fa fd fa fa fa 02 fa fa fa fd fa
=>0x0c0480004a80: fa fa fd fa fa fa 00 00 fa fa 01 fa fa fa[01]fa
  0x0c0480004a90: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c0480004aa0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c0480004ab0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c0480004ac0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c0480004ad0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
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
==28464==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  0x00005555555f3798 in __asan_report_load1 ()
#7  0x00007ffff2a856ad in r_bin_ne_get_entrypoints (bin=<optimized out>) at
#8  0x00007ffff2646680 in r_bin_object_set_items (bf=<optimized out>, bo=<o
#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=<optimized
#13 0x00007ffff384136d in r_core_file_do_load_for_io_plugin (r=0x7fffec2d38
#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 ()
```

```
# sample2
=================================================================
==28366==ERROR: AddressSanitizer: heap-buffer-overflow on ad
READ of size 2 at 0x602000065448 thread T0
    #0 0x7ffff2a85641  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l
```

```
    #1 0x7ffff264667f  (/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+0x270b2)
    #9 0x55555557239d  (/src/cmdline-fuzz/exprs/radare2-5.5.4/radare2+0x1e3

0x602000065448 is located 8 bytes to the left of 1-byte region [0x60200006
allocated by thread T0 here:
    #0 0x5555555ed772  (/src/cmdline-fuzz/exprs/radare2-5.5.4/radare2+0x997
    #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:
  0x0c0480004a30: fa fa 04 fa fa fa 03 fa fa fa 04 fa fa fa 04 fa
  0x0c0480004a40: fa fa 04 fa fa fa fd fa fa fa 07 fa fa fa fd fa
  0x0c0480004a50: fa fa 06 fa fa fa fd fa fa fa 06 fa fa fa fd fa
  0x0c0480004a60: fa fa 06 fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480004a70: fa fa fd fa fa fa fd fa fa fa 02 fa fa fa fd fa
=>0x0c0480004a80: fa fa fd fa fa fa 00 00 fa[fa]01 fa fa fa 00 00
  0x0c0480004a90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004aa0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004ab0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004ac0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004ad0: 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
==28366==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  0x00007ffff2a85642 in r_bin_ne_get_entrypoints (bin=<optimized out>) at
#8  0x00007ffff2646680 in r_bin_object_set_items (bf=<optimized out>, bo=<o
#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=<optimized
#13 0x00007ffff384136d in r_core_file_do_load_for_io_plugin (r=0x7fffec2d38
#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 ()
```



```
# sample3
================================================================
```

```
==28896==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020006
READ of size 2 at 0x602000065670 thread T0
    #0 0x7ffff2a856eb  (/src/cmdline-fuzz/exprs/radare2-5.5.4/src/install/l

    #1 0x7ffff264667f  (/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+0x270b2)
    #9 0x55555557239d  (/src/cmdline-fuzz/exprs/radare2-5.5.4/radare2+0x1e3

0x602000065670 is located 496 bytes to the right of 16-byte region [0x60200
allocated by thread T0 here:
    #0 0x5555555ed772  (/src/cmdline-fuzz/exprs/radare2-5.5.4/radare2+0x997
    #1 0x7ffff2a899ce  (/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:
  0x0c0480004a70: fa fa fd fa fa fa fd fa fa fa 02 fa fa fa fd fa
  0x0c0480004a80: fa fa fd fa fa fa 00 00 fa fa 01 fa fa fa 00 00
  0x0c0480004a90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004aa0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004ab0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c0480004ac0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]fa
  0x0c0480004ad0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004ae0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004af0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004b00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004b10: 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
==28896==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  0x00007ffff2a856ec in r_bin_ne_get_entrypoints (bin=<optimized out>) at
#8  0x00007ffff2646680 in r_bin_object_set_items (bf=<optimized out>, bo=<o
#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=<optimized
#13 0x00007ffff384136d in r_core_file_do_load_for_io_plugin (r=0x7fffec2d38
#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.

References

- PoC Files

CVE
CVE-2022-1238
(Published)

Vulnerability Type
CWE-805: Buffer Access with Incorrect Length Value

Severity
High (7.6)

Registry
Other

Affected Version
5.6.6

Visibility
Public

Status
Fixed

Found by

Han0nly
@han0nly
legend

Fixed by

pancake
@trufae
maintainer

This report was seen 632 times.

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

Han0nly modified the report 8 months ago

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

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 **c40a4f** 8 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

FAQ

contact us

terms

privacy policy

Chat with us