Out of Bounds Read in string_scan_range in radareorg/radare2

0

Valid Reported on May 25th 2022

Description

When providing crafted input, an attacker can cause r_read_32 within string_scan_range to do an out of bounds read. This causes a segmentation fault, but could also potentially enable information disclosure.
What's interesting is there is already a comment stating "may oobread" near this call. I noticed other oob reads occurring that did not cause a segmentation fault.

```
// may oobread
while (needle < to) {
    if (is_breaked && is_breaked ()) {
        break;
    }
    // smol optimization
    if (needle + 4 < to) {
        ut32 n1 = r_read_le32 (buf + needle - from); //crash
        if (!n1) {
            needle += 4;
            continue;
        }
    }
```

ASAN

```
Warning: oobread in LE header parsing relocs
AddressSanitizer:DEADLYSIGNAL
=================================================================
==78927==ERROR: AddressSanitizer: SEGV on unknown address 0x
==78927==The signal is caused by a READ memory access.
```

```
    #0 0x7f025f2dd5eb in r_read_le32 /home/rgood/Projects/radare2/libr/incl
    #1 0x7f025f2dd5eb in string_scan_range /home/rgood/Projects/radare2/lib
    #2 0x7f025f2e469e in get_strings_range /home/rgood/Projects/radare2/lib

    #3 0x7f025f2e50a4 in r_bin_file_get_strings /home/rgood/Projects/radare
    #4 0x7f025f2eb669 in r_bin_object_set_items /home/rgood/Projects/radare
    #5 0x7f025f2ec0bf in r_bin_object_new /home/rgood/Projects/radare2/libr
    #6 0x7f025f2e175a in r_bin_file_new_from_buffer /home/rgood/Projects/ra
    #7 0x7f025f2b6b27 in r_bin_open_buf /home/rgood/Projects/radare2/libr/b
    #8 0x7f025f2b7873 in r_bin_open_io /home/rgood/Projects/radare2/libr/bi
    #9 0x7f025f925237 in r_core_file_do_load_for_io_plugin /home/rgood/Proj
    #10 0x7f025f925237 in r_core_bin_load /home/rgood/Projects/radare2/libr
    #11 0x7f025db3be73 in r_main_radare2 /home/rgood/Projects/radare2/libr/
    #12 0x7f025d95809a in __libc_start_main ../csu/libc-start.c:308
    #13 0x55f2cd30ef49 in _start (/home/rgood/Projects/ASAN-radare2/binr/ra

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/rgood/Projects/radare2/libr/include/r
==78927==ABORTING
```

Backtrace

```
#0  string_scan_range (list=list@entry=0x6030000573d0, bf=bf@entry=0x60d000
    from=from@entry=18446744073709539278, to=to@entry=18446744073709551614,
    section=<optimized out>) at bfile.c:188
#1  0x00007ffff525469f in get_strings_range (bf=0x60d000000ba0, list=<optim
    from=18446744073709539278, to=18446744073709551614, section=<optimized
#2  0x00007ffff52550a5 in r_bin_file_get_strings (bf=bf@entry=0x60d000000ba
    at bfile.c:852
#3  0x00007ffff525b66a in r_bin_object_set_items (bf=bf@entry=0x60d000000ba
#4  0x00007ffff525c0c0 in r_bin_object_new (bf=bf@entry=0x60d000000ba0, plu
    baseaddr=baseaddr@entry=18446744073709551615, loadaddr=loadaddr@entry=0
#5  0x00007ffff525175b in r_bin_file_new_from_buffer (bin=bin@entry=0x61600
    buf=buf@entry=0x6030000552d0, rawstr=<optimized out>, baseaddr=1844674
    fd=<optimized out>, pluginname=<optimized out>) at bfile.c:592
#6  0x00007ffff5226b28 in r_bin_open_buf (bin=bin@entry=0x616000000c80, buf
    at bin.c:285
#7  0x00007ffff5227874 in r_bin_open_io (bin=0x616000000c80,
#8  0x00007ffff5895238 in r_core_file_do_load_for_io_plugin (loadaddr=0, ba
```

```
    at cfile.c:436
#9  r_core_bin_load (r=r@entry=0x7ffff119d800, filenameuri=<optimized out>,
#10 0x00007ffff3aabe74 in r_main_radare2 (argc=<optimized out>, argv=<optim
#11 0x00007ffff38c809b in __libc_start_main (main=0x555555557370 <main>, ar
    fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffde
#12 0x0000555555557f4a in _start ()
```

Proof of Concept

```
radare2 -AA -q oob_read_min_crash_input
```

https://github.com/GreaterGoodest/pocs/blob/master/oob_read_min_crash_input

Impact

Causing DoS and potentially information disclosure.

Occurrences

C bfile.c L187

Call to r_read_le32 results in segfault due to OOB read.

References

- POC

CVE
CVE-2022-1899
(Published)

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

Severity
High (7.7)

Registry

Other

Affected Version
5.6.9

Visibility
Public

Status
Fixed

Found by

Ryan Good
@greatergoodest
legend

Fixed by

pancake
@trufae
maintainer

This report was seen 550 times.

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

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

pancake validated this vulnerability 6 months ago

Ryan Good has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

pancake marked this as fixed in **5.7.0** with commit **193f4f** 6 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

This vulnerability will not receive a CVE ✖

bfile.c#L187 has been validated ✔

Sign in to join this conversation