Heap Buffer Overflow in parseDragons in radareorg/radare2

0

Valid Reported on Mar 23rd 2022

Description

heap buffer overflow in parseDragons function.
ASAN report:

```
=================================================================
==2541037==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200
READ of size 4 at 0x602000065578 thread T0
    #0 0x7f45488bde0c in __interceptor_memcmp ../../../../src/libsanitizer/
    #1 0x7f453cce46b7 in parseDragons /root/radare2/libr/..//libr/bin/p/bin
    #2 0x7f453cce4d6e in load_buffer /root/radare2/libr/..//libr/bin/p/bin_
    #3 0x7f453c8d1d3b in r_bin_object_new /root/radare2/libr/bin/bobj.c:147
    #4 0x7f453c8c6db0 in r_bin_file_new_from_buffer /root/radare2/libr/bin/
    #5 0x7f453c8849f9 in r_bin_open_buf /root/radare2/libr/bin/bin.c:279
    #6 0x7f453c88582e in r_bin_open_io /root/radare2/libr/bin/bin.c:339
    #7 0x7f453ed00223 in r_core_file_do_load_for_io_plugin /root/radare2/li
    #8 0x7f453ed02d77 in r_core_bin_load /root/radare2/libr/core/cfile.c:63
    #9 0x7f454779fb18 in r_main_radare2 /root/radare2/libr/main/radare2.c:1
    #10 0x55eda11bb937 in main /root/radare2/binr/radare2/radare2.c:96
    #11 0x7f4546ba30b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #12 0x55eda11bb30d in _start (/root/radare2/binr/radare2/radare2+0x230d

0x602000065578 is located 1 bytes to the right of 7-byte region [0x60200006
allocated by thread T0 here:
    #0 0x7f45488f0808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x7f453cce456e in parseDragons /root/radare2/libr/..//libr/bin/p/bin
    #2 0x7f453cce4d6e in load_buffer /root/radare2/libr/..//libr/bin/p/bin_
    #3 0x7f453c8d1d3b in r_bin_object_new /root/radare2/libr
    #4 0x7f453c8c6db0 in r_bin_file_new_from_buffer /root/r
    #5 0x7f453c8849f9 in r_bin_open_buf /root/radare2/libr/bin/bin.c:279
```

```
    #6 0x7f453c88582e in r_bin_open_io /root/radare2/libr/bin/bin.c:339
    #7 0x7f453ed00223 in r_core_file_do_load_for_io_plugin /root/radare2/li
    #8 0x7f453ed02d77 in r_core_bin_load /root/radare2/libr/core/cfile.c:63

    #9 0x7f454779fb18 in r_main_radare2 /root/radare2/libr/main/radare2.c:1
    #10 0x55eda11bb937 in main /root/radare2/binr/radare2/radare2.c:96
    #11 0x7f4546ba30b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.

SUMMARY: AddressSanitizer: heap-buffer-overflow ../../../../src/libsanitize
Shadow bytes around the buggy address:
  0x0c0480004a50: fa fa fd fa fa fa 07 fa fa fa fd fa fa fa fd fa
  0x0c0480004a60: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480004a70: fa fa fd fa fa fa 06 fa fa fa fd fa fa fa 06 fa
  0x0c0480004a80: fa fa fd fa fa fa 06 fa fa fa fd fa fa fa fd fa
  0x0c0480004a90: fa fa fd fa fa fa fd fa fa fa fd fa fa fa 02 fa
=>0x0c0480004aa0: fa fa fd fa fa fa fd fa fa fa 00 00 fa fa 07[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
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
  2541027  ABORTING
```

```
==2541037==ABORTING
```

How can we reproduce the issue?

Compile command

```
./sys/sanitize.sh
```

reproduce command
tests_65306.zip

```
unzip tests_65306.zip
./radare2 -qq -AA <poc_file>
```

Impact

latest commit and latest release
$ ./radare2 -v radare2 5.6.6 27858 @ linux-x86-64 git.5.6.2 commit: 50b8813f1df7fbae3bbcb0e8d04397cd353d4759 build: 2022-03-23__02:15:26 $ cat /etc/issue Ubuntu 20.04.3 LTS \n \l

References

- tests_65306.zip

CVE
CVE-2022-1061
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by

peacock-doris

@peacock-doris

unranked

Fixed by

pancake

@trufae

maintainer

This report was seen 672 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 validated this vulnerability 8 months ago

peacock-doris 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 **d4ce40** 8 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation