# Heap Buffer Overflow in iterate_chained_fixups in radareorg/radare2

0

Valid Reported on Mar 22nd 2022

## Description

heap buffer overflow in iterate_chained_fixups function.
ASAN report:

```
=================================================================
==2540511==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200
READ of size 8 at 0x602000065710 thread T0
    #0 0x7f5b64ccb877 in iterate_chained_fixups /root/radare2/libr/..//libr
    #1 0x7f5b64c77396 in rebase_buffer /root/radare2/libr/..//libr/bin/p/bi
    #2 0x7f5b64c76cd2 in rebasing_and_stripping_io_read /root/radare2/libr/
    #3 0x7f5b6e4aa493 in r_io_plugin_read /root/radare2/libr/io/io_plugin.c
    #4 0x7f5b6e4b3d19 in r_io_desc_read /root/radare2/libr/io/io_desc.c:213
    #5 0x7f5b6e4c708c in r_io_fd_read /root/radare2/libr/io/io_fd.c:24
    #6 0x7f5b6ffa0369 in buf_io_read /root/radare2/libr/util/buf_io.c:72
    #7 0x7f5b6ffa1fc2 in buf_read /root/radare2/libr/util/buf.c:46
    #8 0x7f5b6ffa5ef3 in r_buf_read /root/radare2/libr/util/buf.c:452
    #9 0x7f5b6ffa7259 in r_buf_read_at /root/radare2/libr/util/buf.c:600
    #10 0x7f5b64ccafb8 in get_hdr /root/radare2/libr/..//libr/bin/p/../form
    #11 0x7f5b64cca3dc in mach_fields /root/radare2/libr/..//libr/bin/p/../
    #12 0x7f5b64aa04a1 in r_bin_object_set_items /root/radare2/libr/bin/bob
    #13 0x7f5b64a9d2a6 in r_bin_object_new /root/radare2/libr/bin/bobj.c:16
    #14 0x7f5b64a91db0 in r_bin_file_new_from_buffer /root/radare2/libr/bin
    #15 0x7f5b64a4f9f9 in r_bin_open_buf /root/radare2/libr/bin/bin.c:279
    #16 0x7f5b64a5082e in r_bin_open_io /root/radare2/libr/bin/bin.c:339
    #17 0x7f5b66ecb223 in r_core_file_do_load_for_io_plugin /root/radare2/l
    #18 0x7f5b66ecdd77 in r_core_bin_load /root/radare2/libr/core/cfile.c:6
    #19 0x7f5b6f96ab18 in r_main_radare2 /root/radare2/libr/
    #20 0x564e0b55f937 in main /root/radare2/binr/radare2/r
    #21 0x7f5b6ed6e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
```

```
    #22 0x564e0b55f30d in _start (/root/radare2/binr/radare2/radare2+0x230d

0x602000065711 is located 0 bytes to the right of 1-byte region [0x6020000657

allocated by thread T0 here:
    #0 0x7f5b70abba06 in __interceptor_calloc ../../../../src/libsanitizer/
    #1 0x7f5b64c96f4b in parse_chained_fixups /root/radare2/libr/..//libr/bi
    #2 0x7f5b64ca2b6b in init_items /root/radare2/libr/..//libr/bin/p/../fo
    #3 0x7f5b64ca2f29 in init /root/radare2/libr/..//libr/bin/p/../format/m
    #4 0x7f5b64ca55fa in new_buf /root/radare2/libr/..//libr/bin/p/../formc
    #5 0x7f5b64c6a112 in load_buffer /root/radare2/libr/..//libr/bin/p/bin_
    #6 0x7f5b64a9cd3b in r_bin_object_new /root/radare2/libr/bin/bobj.c:147
    #7 0x7f5b64a91db0 in r_bin_file_new_from_buffer /root/radare2/libr/bin/
    #8 0x7f5b64a4f9f9 in r_bin_open_buf /root/radare2/libr/bin/bin.c:279
    #9 0x7f5b64a5082e in r_bin_open_io /root/radare2/libr/bin/bin.c:339
    #10 0x7f5b66ecb223 in r_core_file_do_load_for_io_plugin /root/radare2/li
    #11 0x7f5b66ecdd77 in r_core_bin_load /root/radare2/libr/core/cfile.c:68
    #12 0x7f5b6f96ab18 in r_main_radare2 /root/radare2/libr/main/radare2.c:1
    #13 0x564e0b55f937 in main /root/radare2/binr/radare2/radare2.c:96
    #14 0x7f5b6ed6e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/radare2/libr/..//libr
Shadow bytes around the buggy address:
  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 00 02
  0x0c0480004ab0: fa fa 00 02 fa fa 02 fa fa fa 05 fa fa fa 05 fa
  0x0c0480004ac0: fa fa 00 00 fa fa 00 02 fa fa 05 fa fa fa 00 06
  0x0c0480004ad0: fa fa 00 00 fa fa 00 fa fa fa 05 fa fa fa 02 fa
=>0x0c0480004ae0: fa fa[01]fa fa fa 05 fa fa fa 07 fa fa fa 00 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
  0x0c0480004b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480004b30: 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
==2540511==ABORTING
```

## How can we reproduce the issue?

Compile command

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

reproduce command
tests_65305.zip

```
unzip tests_65305.zip
./radare2 -qq -AA <poc_file>
```

## Impact

latest commit and latest release
$ ./radare2 -v radare2 5.6.5 27847 @ linux-x86-64 git.5.6.2 commit: 60182bb63a77282ae469654556b899dbe2a7674c build: 2022-03-22__09:29:41 $ cat /etc/issue Ubuntu 20.04.3 LTS \n \l

## References

- tests_65305.zip

CVE
CVE-2022-1052
(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 663 times.

We are processing your report and will contact the **radareorg/radare2** team within 24 hours.
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 **5.6.6** with commit **005250** 8 months ago

**pancake** has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ×

Sign in to join this conversation