Heap-based Buffer Overflow in radareorg/radare2

0

Valid Reported on May 11th 2022

Description

Heap-based Buffer Overflow in msp430_op

Environment

```
radare2 5.6.9 0 @ linux-x86-64 git.
commit: 5.6.9 build: 2022-05-01__12:17:49
```

Build

```
export CC=gcc CXX=g++ CFLAGS="-fsanitize=address -static-libasan" CXXFLAGS=
./configure && make
```

POC

```
radare2 -q -A ./poc6
```

poc6

Asan

```
=================================================================
==4030479==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200
READ of size 1 at 0x6020000595d3 thread T0
    #0 0x7f2b12c8cfa5 in r_read_le16 /home/ubuntu/radare2-master/libr/incl
    #1 0x7f2b12c8cfa5 in r_read_at_le16 /home/ubuntu/radare2-master/libr/ir
```

```
    #2 0x7f2b12c8cfa5 in msp430_op /home/ubuntu/radare2-master/libr/../lib
    #3 0x7f2b12de2d19 in r_anal_op /home/ubuntu/radare2-master/libr/anal/op
    #4 0x7f2b14f241df in anal_block_cb /home/ubuntu/radare2-master/libr/cor
    #5 0x7f2b12e267e8 in r_anal_block_recurse_depth_first /home/ubuntu/rada
    #6 0x7f2b14f565fd in r_core_recover_vars /home/ubuntu/radare2-master/li
    #7 0x7f2b14bcd43f in r_core_af /home/ubuntu/radare2-master/libr/core/cm
    #8 0x7f2b14f5e320 in r_core_anal_all /home/ubuntu/radare2-master/libr/c
    #9 0x7f2b14cac9e6 in cmd_anal_all /home/ubuntu/radare2-master/libr/core
    #10 0x7f2b14d1aadc in cmd_anal /home/ubuntu/radare2-master/libr/core/cm
    #11 0x7f2b14c08d2c in r_core_cmd_subst_i /home/ubuntu/radare2-master/li
    #12 0x7f2b14c08d2c in r_core_cmd_subst /home/ubuntu/radare2-master/libr
    #13 0x7f2b14c1682a in run_cmd_depth /home/ubuntu/radare2-master/libr/co
    #14 0x7f2b14c1682a in r_core_cmd /home/ubuntu/radare2-master/libr/core/
    #15 0x7f2b14c1682a in r_core_cmd /home/ubuntu/radare2-master/libr/core/
    #16 0x7f2b17aee546 in r_main_radare2 /home/ubuntu/radare2-master/libr/m
    #17 0x7f2b178900b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #18 0x564ce9a25b6d in _start (/home/ubuntu/radare2-master/binr/radare2/

0x6020000595d3 is located 1 bytes to the right of 2-byte region [0x60200005
allocated by thread T0 here:
    #0 0x564ce9b10bb8 in __interceptor_malloc (/home/ubuntu/radare2-master/
    #1 0x7f2b14f23c9b in anal_block_cb /home/ubuntu/radare2-master/libr/cor

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/ubuntu/radare2-master
Shadow bytes around the buggy address:
  0x0c0480003260: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480003270: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480003280: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480003290: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c04800032a0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
=>0x0c04800032b0: fa fa fd fa fa fa fd fa fa fa[02]fa fa fa fa fa
  0x0c04800032c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800032d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800032e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c04800032f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0480003300: 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
==4030479==ABORTING
```

Impact

The bug causes the program reads data past the end of the intented buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.

CVE
CVE-2022-1714
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.9)

Registry
Other

Affected Version
5.6.9

Visibility
Public

Status
Fixed

Found by

cnitlrt
@cnitlrt
master

Fixed by

pancake
@trufae
maintainer

This report was seen 504 times.

We are processing your report and will contact the **radareorg/radare2** team within 24 hours.
7 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

cnitlrt 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 **3ecdbf** 6 months ago

pancake has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

Chat with us