Heap-buffer-overflow in UnsetPending #84

Open liyansong2018 opened this issue on Jun 25 · 0 comments

liyansong2018 commented on Jun 25 • edited

Hi :)

When I was decompiling the Lua script on openwrt, I found a `segmentation fault` error. I try to debug luadec to find the location of bug. Size of some array variables in function structure is 255. However, these variables were accessed out of bounds in decompiling.

```
#define MAXARG_A        ((1<<SIZE_A)-1)    // 255

/* Function structure in /home/lys/Tools/luadec/luadec/decompile.h*/
/* These act as the VM registers */
char* R[MAXARG_A];
/* These store the priority for the operation that stored the value in each
register */
int Rprio[MAXARG_A];
/* Boolean values indicating if register holds a table */
int Rtabl[MAXARG_A];
/* Registers standing for local variables. */
int Rvar[MAXARG_A];
/* Pending code to be flushed */
int Rpend[MAXARG_A];
/* Registers for internal use */
int Rinternal[MAXARG_A];
/* Registers used in call returns */
int Rcall[MAXARG_A];
```

Below is the log.

```
$ /home/lys/Tools/luadec/luadec/luadec sys.lua
cannot find blockend > 251 , pc = 250, f->sizecode = 252
cannot find blockend > 252 , pc = 251, f->sizecode = 252
cannot find blockend > 6 , pc = 5, f->sizecode = 7
cannot find blockend > 7 , pc = 6, f->sizecode = 7
cannot find blockend > 63 , pc = 62, f->sizecode = 64
cannot find blockend > 64 , pc = 63, f->sizecode = 64
```

```
cannot find blockend > 20 , pc = 19, f->sizecode = 21
cannot find blockend > 21 , pc = 20, f->sizecode = 21
cannot find blockend > 37 , pc = 36, f->sizecode = 38
cannot find blockend > 38 , pc = 37, f->sizecode = 38
cannot find blockend > 10 , pc = 9, f->sizecode = 11
cannot find blockend > 11 , pc = 10, f->sizecode = 11
cannot find blockend > 5 , pc = 4, f->sizecode = 6
cannot find blockend > 6 , pc = 5, f->sizecode = 6
cannot find blockend > 94 , pc = 93, f->sizecode = 95
cannot find blockend > 95 , pc = 94, f->sizecode = 95
cannot find blockend > 6 , pc = 5, f->sizecode = 7
cannot find blockend > 7 , pc = 6, f->sizecode = 7
cannot find blockend > 6 , pc = 5, f->sizecode = 7
cannot find blockend > 7 , pc = 6, f->sizecode = 7
cannot find blockend > 13 , pc = 12, f->sizecode = 14
cannot find blockend > 14 , pc = 13, f->sizecode = 14
cannot find blockend > 5 , pc = 4, f->sizecode = 6
cannot find blockend > 6 , pc = 5, f->sizecode = 6
cannot find blockend > 54 , pc = 53, f->sizecode = 55
cannot find blockend > 55 , pc = 54, f->sizecode = 55
cannot find blockend > 196 , pc = 195, f->sizecode = 197
cannot find blockend > 197 , pc = 196, f->sizecode = 197
cannot find blockend > 61 , pc = 60, f->sizecode = 62
cannot find blockend > 62 , pc = 61, f->sizecode = 62
cannot find blockend > 16 , pc = 15, f->sizecode = 17
cannot find blockend > 17 , pc = 16, f->sizecode = 17
cannot find blockend > 18 , pc = 17, f->sizecode = 19
cannot find blockend > 19 , pc = 18, f->sizecode = 19
cannot find blockend > 33 , pc = 32, f->sizecode = 34
cannot find blockend > 34 , pc = 33, f->sizecode = 34
cannot find blockend > 38 , pc = 37, f->sizecode = 39
cannot find blockend > 39 , pc = 38, f->sizecode = 39
cannot find blockend > 18 , pc = 17, f->sizecode = 19
cannot find blockend > 19 , pc = 18, f->sizecode = 19
cannot find blockend > 19 , pc = 18, f->sizecode = 20
cannot find blockend > 20 , pc = 19, f->sizecode = 20
cannot find blockend > 24 , pc = 23, f->sizecode = 25
cannot find blockend > 25 , pc = 24, f->sizecode = 25
cannot find blockend > 18 , pc = 17, f->sizecode = 19
cannot find blockend > 19 , pc = 18, f->sizecode = 19
cannot find blockend > 19 , pc = 18, f->sizecode = 20
cannot find blockend > 20 , pc = 19, f->sizecode = 20
cannot find blockend > 24 , pc = 23, f->sizecode = 25
cannot find blockend > 25 , pc = 24, f->sizecode = 25
cannot find blockend > 93 , pc = 92, f->sizecode = 94
cannot find blockend > 94 , pc = 93, f->sizecode = 94
cannot find blockend > 6 , pc = 5, f->sizecode = 7
cannot find blockend > 7 , pc = 6, f->sizecode = 7
cannot find blockend > 14 , pc = 13, f->sizecode = 15
cannot find blockend > 15 , pc = 14, f->sizecode = 15
cannot find blockend > 20 , pc = 19, f->sizecode = 21
cannot find blockend > 21 , pc = 20, f->sizecode = 21
cannot find blockend > 17 , pc = 16, f->sizecode = 18
cannot find blockend > 18 , pc = 17, f->sizecode = 18
cannot find blockend > 15 , pc = 14, f->sizecode = 16
cannot find blockend > 16 , pc = 15, f->sizecode = 16
```

```
cannot find blockend > 17 , pc = 16, f->sizecode = 18
cannot find blockend > 18 , pc = 17, f->sizecode = 18
cannot find blockend > 42 , pc = 41, f->sizecode = 43
cannot find blockend > 43 , pc = 42, f->sizecode = 43
cannot find blockend > 7 , pc = 6, f->sizecode = 8
cannot find blockend > 8 , pc = 7, f->sizecode = 8
cannot find blockend > 6 , pc = 5, f->sizecode = 7
cannot find blockend > 7 , pc = 6, f->sizecode = 7
cannot find blockend > 90 , pc = 89, f->sizecode = 91
cannot find blockend > 91 , pc = 90, f->sizecode = 91
cannot find blockend > 118 , pc = 117, f->sizecode = 119
cannot find blockend > 119 , pc = 118, f->sizecode = 119
cannot find blockend > 11 , pc = 10, f->sizecode = 12
cannot find blockend > 12 , pc = 11, f->sizecode = 12
cannot find blockend > 13 , pc = 12, f->sizecode = 14
cannot find blockend > 14 , pc = 13, f->sizecode = 14
cannot find blockend > 15 , pc = 14, f->sizecode = 16
cannot find blockend > 16 , pc = 15, f->sizecode = 16
cannot find blockend > 34 , pc = 33, f->sizecode = 35
cannot find blockend > 35 , pc = 34, f->sizecode = 35
cannot find blockend > 5 , pc = 4, f->sizecode = 6
cannot find blockend > 6 , pc = 5, f->sizecode = 6
cannot find blockend > 5 , pc = 4, f->sizecode = 6
cannot find blockend > 6 , pc = 5, f->sizecode = 6
cannot find blockend > 36 , pc = 35, f->sizecode = 37
cannot find blockend > 37 , pc = 36, f->sizecode = 37
cannot find blockend > 20 , pc = 19, f->sizecode = 21
cannot find blockend > 21 , pc = 20, f->sizecode = 21
cannot find blockend > 27 , pc = 26, f->sizecode = 28
cannot find blockend > 28 , pc = 27, f->sizecode = 28
cannot find blockend > 65 , pc = 64, f->sizecode = 66
cannot find blockend > 66 , pc = 65, f->sizecode = 66
cannot find blockend > 18 , pc = 17, f->sizecode = 19
cannot find blockend > 19 , pc = 18, f->sizecode = 19
cannot find blockend > 11 , pc = 10, f->sizecode = 12
cannot find blockend > 12 , pc = 11, f->sizecode = 12
cannot find blockend > 14 , pc = 13, f->sizecode = 15
cannot find blockend > 15 , pc = 14, f->sizecode = 15
cannot find blockend > 19 , pc = 18, f->sizecode = 20
cannot find blockend > 20 , pc = 19, f->sizecode = 20
cannot find blockend > 18 , pc = 17, f->sizecode = 19
cannot find blockend > 19 , pc = 18, f->sizecode = 19
cannot find blockend > 19 , pc = 18, f->sizecode = 20
cannot find blockend > 20 , pc = 19, f->sizecode = 20
cannot find blockend > 9 , pc = 8, f->sizecode = 10
cannot find blockend > 10 , pc = 9, f->sizecode = 10
cannot find blockend > 9 , pc = 8, f->sizecode = 10
cannot find blockend > 10 , pc = 9, f->sizecode = 10
cannot find blockend > 9 , pc = 8, f->sizecode = 10
cannot find blockend > 10 , pc = 9, f->sizecode = 10
cannot find blockend > 9 , pc = 8, f->sizecode = 10
cannot find blockend > 10 , pc = 9, f->sizecode = 10
cannot find blockend > 9 , pc = 8, f->sizecode = 10
cannot find blockend > 10 , pc = 9, f->sizecode = 10
cannot find blockend > 54 , pc = 53, f->sizecode = 55
cannot find blockend > 55 , pc = 54, f->sizecode = 55
```

```
-- Decompiled using luadec 2.2 rev: c2903eb for Lua 5.1 from https://github.com/viruscamp/luadec
-- Command line: sys.lua

processing OP_JMP to } else {
 at line 2649 in file decompile.c
 for lua files: sys.lua
 at lua function 0_3 pc=21

=================================================================
==1879041==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62500000e9f8 at pc 0x562ba0ab25
READ of size 4 at 0x62500000e9f8 thread T0
    #0 0x562ba0ab2565 in UnsetPending /home/lys/Tools/luadec/luadec/decompile.c:964
    #1 0x562ba0ab5f3e in GetR /home/lys/Tools/luadec/luadec/decompile.c:1101
    #2 0x562ba0ab6529 in SetList /home/lys/Tools/luadec/luadec/decompile.c:944
    #3 0x562ba0abde6e in ProcessCode /home/lys/Tools/luadec/luadec/decompile.c:3029
    #4 0x562ba0ac0907 in ProcessCode /home/lys/Tools/luadec/luadec/decompile.c:3137
    #5 0x562ba0ac3340 in luaU_decompile /home/lys/Tools/luadec/luadec/decompile.c:3207
    #6 0x562ba0aa80ad in main /home/lys/Tools/luadec/luadec/luadec.c:485
    #7 0x7f30e4e627ec in __libc_start_main ../csu/libc-start.c:332
    #8 0x562ba0aa8999 in _start (/home/lys/Tools/luadec/luadec/luadec+0x11999)

0x62500000e9f8 is located 0 bytes to the right of 8440-byte region [0x62500000c900,0x62500000e9f8)
allocated by thread T0 here:
    #0 0x7f30e51f5987 in __interceptor_calloc ../../../../src/libsanitizer/asan/asan_malloc_linux.cpp
    #1 0x562ba0ab369b in NewFunction /home/lys/Tools/luadec/luadec/decompile.c:1039

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/lys/Tools/luadec/luadec/decompile.c:964 in Unse
Shadow bytes around the buggy address:
  0x0c4a7fff9ce0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fff9cf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fff9d00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fff9d10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fff9d20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c4a7fff9d30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]
  0x0c4a7fff9d40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff9d50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff9d60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff9d70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff9d80: 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
==1879041==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant