jerryscript-project / **jerryscript** Public

Code  Issues 71  Pull requests 39  Actions  Wiki  Security  ···

New issue

Jump to bottom

# Stack-buffer-overflow in jerryx_print_unhandled_exception (jerryscript/jerry-ext/util/print.c) #5008

Closed  **paintedveil5** opened this issue on May 29 · 1 comment · Fixed by #5012

**paintedveil5** commented on May 29 • edited

###### JerryScript revision

`0d49696`
master

###### Build platform

Ubuntu 16.04.7 LTS (Linux 4.15.0-142-generic x86_64)

###### Build steps

```
./tools/build.py --clean --compile-flag=-fsanitize=address --lto=off --error-message=on --profile=es.
```

###### Test case

```
for (let __v1 = 0; __v1 < 10000; __v1++) {
    ['__v6', '__v2', '__v1', '__v3', '__v4', '__v5'];"    __v5(__v1,
}
```

```
==112046==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffda03d5390 at pc 0x7fa6aae1ea
READ of size 1 at 0x7ffda03d5390 thread T0
    #0 0x7fa6aae1ea7c in __interceptor_strtol (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x75a7c)
    #1 0x581203 in jerryx_print_unhandled_exception /home/lily/Desktop/67/jerryscript/jerry-ext/util/
    #2 0x4027c1 in main /home/lily/Desktop/67/jerryscript/jerry-main/main-desktop.c:172
    #3 0x7fa6aa6f683f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #4 0x401e88 in _start (/home/lily/Desktop/67/jerry+0x401e88)

Address 0x7ffda03d5390 is located in stack of thread T0 at offset 224 in frame
```

```
    #0 0x580e99 in jerryx_print_unhandled_exception /home/lily/Desktop/67/jerryscript/jerry-ext/util/

  This frame has 3 object(s):
    [32, 36) 'source_size'
    [96, 104) 'current_p'
    [160, 224) 'buffer_p' <== Memory access at offset 224 overflows this variable
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swapcon
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow ??:0 __interceptor_strtol
Shadow bytes around the buggy address:
  0x100034072a20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100034072a30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100034072a40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100034072a50: 00 00 00 00 00 00 f1 f1 f1 f1 04 f4 f4 f4 f2 f2
  0x100034072a60: f2 f2 00 f4 f4 f4 f2 f2 f2 f2 00 00 00 00 00 00
=>0x100034072a70: 00 00[f3]f3 f3 f3 f3 f3 f3 f3 00 00 00 00 00 00
  0x100034072a80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100034072a90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100034072aa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100034072ab0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100034072ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==112046==ABORTING
```

**zherczeg** mentioned this issue on Jul 22

Fix exception printing. #5012

Merged

**zherczeg** commented on Jul 22 Member

The exception printing did not detect the end of stream. You can also increase the printing buffer size from 63 byte if you need these longer messages.

**robertsipka** closed this as completed in #5012 on Aug 8

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

**Fix exception printing.**
zherczeg/jerryscript

2 participants