Segmentation fault in lj_err_run #601

Closed **Changochen** opened this issue on Jul 10, 2020 · 4 comments

Labels 2.0 2.1 bug

Changochen commented on Jul 10, 2020

Hi, we found a crash in LuaJit

Version: 2.1. Git hash: `384d6d56f4a3841fdef607a511dda92a579af2ff`

POC:

```
a = newproxy ( true )
getmetatable ( a ) . __gc = function ( )
    rep129 = load ( function ( ) collectgarbage ( )  (  )   end )
end
for i = 1 , 10000000 do   newproxy ( a ) end
```

Stack dump:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==3119==ERROR: AddressSanitizer: SEGV on unknown address 0x7fe86c68800c (pc 0x0000004c7779 bp 0x7ffcaa608950 sp 0x7ffcaa6087c0 T0)
==3119==The signal is caused by a READ memory access.
    #0 0x4c7778 in lj_err_run /home/yongheng/LuaJit_asan/src/lj_err.c:607:10
    #1 0x4c7b34 in err_msgv /home/yongheng/LuaJit_asan/src/lj_err.c:631:3
    #2 0x4c7ec1 in lj_err_optype /home/yongheng/LuaJit_asan/src/lj_err.c:667:3
    #3 0x4c8040 in lj_err_optype_call /home/yongheng/LuaJit_asan/src/lj_err.c:695:3
    #4 0x55d32e in lj_meta_call /home/yongheng/LuaJit_asan/src/lj_meta.c:442:5
    #5 0x548fcc in lj_vmeta_call (/home/yongheng/LuaJit_asan/src/luajit+0x548fcc)
    #6 0x611efc in reader_func /home/yongheng/LuaJit_asan/src/lib_base.c:390:3
    #7 0x4f9fa3 in lex_more /home/yongheng/LuaJit_asan/src/lj_lex.c:49:19
    #8 0x4f5580 in lex_next /home/yongheng/LuaJit_asan/src/lj_lex.c:65:65
    #9 0x4f5580 in lj_lex_setup /home/yongheng/LuaJit_asan/src/lj_lex.c:418:3
    #10 0x522a4e in cpparser /home/yongheng/LuaJit_asan/src/lj_load.c:36:8
    #11 0x548baa in lj_vm_cpcall (/home/yongheng/LuaJit_asan/src/luajit+0x548baa)
    #12 0x5228dc in lua_loadx /home/yongheng/LuaJit_asan/src/lj_load.c:58:12
    #13 0x6110c0 in lj_cf_load /home/yongheng/LuaJit_asan/src/lib_base.c:417:14
    #14 0x5487b4 in lj_BC_FUNCC (/home/yongheng/LuaJit_asan/src/luajit+0x5487b4)
    #15 0x54ba14 in gc_call_finalizer /home/yongheng/LuaJit_asan/src/lj_gc.c:511:13
    #16 0x54b3da in gc_finalize /home/yongheng/LuaJit_asan/src/lj_gc.c:558:5
    #17 0x54d241 in gc_onestep /home/yongheng/LuaJit_asan/src/lj_gc.c:696:7
    #18 0x54e727 in lj_gc_fullgc /home/yongheng/LuaJit_asan/src/lj_gc.c:786:8
    #19 0x4f463c in lua_gc /home/yongheng/LuaJit_asan/src/lj_api.c:1256:5
    #20 0x611571 in lj_cf_collectgarbage /home/yongheng/LuaJit_asan/src/lib_base.c:455:15
    #21 0x5487b4 in lj_BC_FUNCC (/home/yongheng/LuaJit_asan/src/luajit+0x5487b4)
    #22 0x611efc in reader_func /home/yongheng/LuaJit_asan/src/lib_base.c:390:3
    #23 0x4f9fa3 in lex_more /home/yongheng/LuaJit_asan/src/lj_lex.c:49:19
    #24 0x4f5580 in lex_next /home/yongheng/LuaJit_asan/src/lj_lex.c:65:65
    #25 0x4f5580 in lj_lex_setup /home/yongheng/LuaJit_asan/src/lj_lex.c:418:3
    #26 0x522a4e in cpparser /home/yongheng/LuaJit_asan/src/lj_load.c:36:8
    #27 0x548baa in lj_vm_cpcall (/home/yongheng/LuaJit_asan/src/luajit+0x548baa)
    #28 0x5228dc in lua_loadx /home/yongheng/LuaJit_asan/src/lj_load.c:58:12
    #29 0x6110c0 in lj_cf_load /home/yongheng/LuaJit_asan/src/lib_base.c:417:14
    #30 0x5487b4 in lj_BC_FUNCC (/home/yongheng/LuaJit_asan/src/luajit+0x5487b4)
    #31 0x54ba14 in gc_call_finalizer /home/yongheng/LuaJit_asan/src/lj_gc.c:511:13
    #32 0x54b3da in gc_finalize /home/yongheng/LuaJit_asan/src/lj_gc.c:558:5
    #33 0x54d241 in gc_onestep /home/yongheng/LuaJit_asan/src/lj_gc.c:696:7
    #34 0x54c367 in lj_gc_step /home/yongheng/LuaJit_asan/src/lj_gc.c:726:20
    #35 0x4eddaf in lua_newuserdata /home/yongheng/LuaJit_asan/src/lj_api.c:759:3
    #36 0x611669 in lj_cf_newproxy /home/yongheng/LuaJit_asan/src/lib_base.c:471:3
    #37 0x5487b4 in lj_BC_FUNCC (/home/yongheng/LuaJit_asan/src/luajit+0x5487b4)
    #38 0x4f3426 in lua_pcall /home/yongheng/LuaJit_asan/src/lj_api.c:1140:12
    #39 0x4c60f4 in docall /home/yongheng/LuaJit_asan/src/luajit.c:121:12
    #40 0x4c5790 in handle_script /home/yongheng/LuaJit_asan/src/luajit.c:292:14
    #41 0x4c5790 in pmain /home/yongheng/LuaJit_asan/src/luajit.c:553:17
    #42 0x5487b4 in lj_BC_FUNCC (/home/yongheng/LuaJit_asan/src/luajit+0x5487b4)
    #43 0x4f350e in lua_cpcall /home/yongheng/LuaJit_asan/src/lj_api.c:1165:12
    #44 0x4c4ab1 in main /home/yongheng/LuaJit_asan/src/luajit.c:582:12
    #45 0x7fe86f40e82f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/../csu/libc-start.c:291
    #46 0x41d4c8 in _start (/home/yongheng/LuaJit_asan/src/luajit+0x41d4c8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/yongheng/LuaJit_asan/src/lj_err.c:607:10 in lj_err_run
```

Mike **MikePall** added 2.0 2.1 bug labels on Jul 12, 2020

MikePall commented on Jul 12, 2020 Member

Fixed. Thanks!

Mike **MikePall** closed this as completed on Jul 12, 2020

galaktipus commented on Jul 23, 2020

I see CVE-2020-15890 was assigned. Any commit for the issue?

MikePall commented on Jul 27, 2020 Member

Look for `__gc` in the commit history.

Recently, it has become some kind of sport to file nonsensical and mean-spirited CVEs against LuaJIT. I'm sick of filing take-down notices and will just ignore this one.

This one in particular isn't even worth assigning a CVE. The `__gc` metamethod is only invoked on userdata. And if you let untrusted code modify the metamethods of userdata objects you're toast, anyway. Likewise, `newproxy` should never be accessible in any sandbox. See also the FAQ entry on sandboxes: https://luajit.org/faq.html#sandbox

This was referenced on Jul 27, 2020

Vulnerability roundup 90: luajit-2.1.0-beta3: 1 advisory [7.5] NixOS/nixpkgs#93997

Closed

Vulnerability roundup 90: luajit-2.0.5: 1 advisory [7.5] NixOS/nixpkgs#94002

Closed

ncopa commented on Aug 18, 2020

This looks like the commit: `53f82e6`

Assignees

No one assigned

Labels

2.0 2.1 bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants