lua-users
lua-l archive

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

- **Subject**: **Stack overflow in luaO_pushvfstring**
- **From**: Yongheng Chen <changochen1@...>
- **Date**: Mon, 6 Jul 2020 00:27:48 -0400

Hi,

We found a stack overflow in lua. Here’s the details:

Version:

Lua 5.4.0, git hash c33b1728aeb7dfeec4013562660e07d32697aa6b

POC:

```
function errfunc() xpcall(function() print(xpcall(test, errfunc)) end, errfunc)
  end(function() print(xpcall(test, errfunc)) end)()
```

How to reproduce:

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

Stack dump:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==16336==ERROR: AddressSanitizer: stack-overflow on address 0x7fffad2a9d78 (pc 0x7f9977ca3796 bp 0x7fffad2aa610 sp 0x7fffad2a9d80 T0)
  #0 0x7f9977ca3795  (/usr/lib/x86_64-linux-gnu/libasan.so.5+0x73795)
  #1 0x422a0c in luaO_pushvfstring (/home/yongheng/lua_asan/lua+0x422a0c)
  #2 0x411455 in luaG_runerror (/home/yongheng/lua_asan/lua+0x411455)
  #3 0x411595 in luaG_typeerror (/home/yongheng/lua_asan/lua+0x411595)
  #4 0x4138bc in luaD_tryfuncTM (/home/yongheng/lua_asan/lua+0x4138bc)
  #5 0x41480d in luaD_call (/home/yongheng/lua_asan/lua+0x41480d)
  #6 0x415194 in luaD_callnoyield (/home/yongheng/lua_asan/lua+0x415194)
  #7 0x4127d0 in luaD_rawrunprotected (/home/yongheng/lua_asan/lua+0x4127d0)
  #8 0x415d70 in luaD_pcall (/home/yongheng/lua_asan/lua+0x415d70)
  #9 0x40bd47 in lua_pcallk (/home/yongheng/lua_asan/lua+0x40bd47)
  #10 0x45672e in luaB_xpcall (/home/yongheng/lua_asan/lua+0x45672e)
 #11 0x414de1 in luaD_call (/home/yongheng/lua_asan/lua+0x414de1)
 ….
```

Found by: Yongheng Chen and Rui Zhong

Best,

Yongheng

Sent from Mail for Windows 10

- **Follow-Ups**:
  - **Re: Stack overflow in luaO_pushvfstring**, *Luiz Henrique de Figueiredo*
  - **Re: Stack overflow in luaO_pushvfstring**, *Roberto Ierusalimschy*

- Prev by Date: **[ANN] Ravi (a Lua dialect) 1.0 Beta-4 Release with JIT compilation support**
- Next by Date: **Heap use after free in luaD_call**
- Previous by thread: **Re: [ANN] Ravi (a Lua dialect) 1.0 Beta-4 Release with JIT compilation support**
- Next by thread: **Re: Stack overflow in luaO_pushvfstring**
- Index(es):
  - **Date**
  - **Thread**