- **Subject**: **Segmentation fault in changedline**
- **From**: Yongheng Chen <changochen1@...>
- **Date**: Thu, 9 Jul 2020 18:03:49 -0400

Hi,

We found a segmentation fault in changedline, called by luaG_traceexec.

Version:

Lua 5.4.0, git hash 31b8c2d4380a762d1ed6a7faee74a1d107f86014

Tested on default build of lua on Ubuntu 18. If we build with asan, the error is gone.

An already-reduced POC:

```
function errfunc ( p1, p2, p3, p12, p13, p14, p15, p6, p7, p16, p18, p19, p20, p21,
  p22, p23, p24, 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 )
  return end
  function test (  )
    print ( do_yield and "" )
    pcall ( function (  )if do_yield then end end )
    error 'fail' end coro =
    coroutine.wrap ( function (  )print ( xpcall ( test, errfunc, false ) )
      do
        k = 0 local x::foo::assert ( not y ) k =
        1 if k then function g (  )setmetatable (
          {
          }
          ,
          {
            __gc = function() function errfunc(x) end function test(do_yield) print
            "yieldingnot yielding" pcall(function() if do_yield then yield() end end)
            error 'fail' end
            coro = coroutine.wrap coro() string.char(
            0, 'BCDEFGHIJKLMNOPQRSTUVWXYZ'..'abcdefghijklmnopqrstuvwxyz',
            "")(function() yield() end) end
          }
          ) end
          function f (  )
            debug.sethook ( print, "l" ) for j =
            1, 1000
            do
              g (  )
            end
          end
          f (  )
        end
      end
    end )
    (  )
```

---

Partial Stackdump:

```
#0  0x00000000004248b3 in changedline (newpc=0x5, oldpc=0xffffe4b5, p=0xf84380)
    at ldebug.c:791
#1  luaG_traceexec (L=0xf846b8, pc=0xf86d08) at ldebug.c:826
#2  0x00000000004923f5 in luaV_execute (L=L@entry=0xf846b8, ci=<optimized out>)
    at lvm.c:1725
#3  0x000000000042e792 in luaD_call (L=L@entry=0xf846b8, func=<optimized out>,
    nresults=<optimized out>) at ldo.c:504
#4  0x00000000004973ab in luaV_execute (L=L@entry=0xf846b8, ci=<optimized out>)
    at lvm.c:1614
#5  0x000000000042e792 in luaD_call (L=L@entry=0xf846b8, func=<optimized out>,
    nresults=<optimized out>) at ldo.c:504
#6  0x00000000004973ab in luaV_execute (L=L@entry=0xf846b8, ci=ci@entry=0xf84a20)
    at lvm.c:1614
#7  0x000000000042be7c in unroll (ud=0x7fff48258edc, L=0xf846b8) at ldo.c:574
#8  luaD_rawrunprotected (L=L@entry=0xf846b8, ud=ud@entry=0x7fff48258edc,
    f=<optimized out>) at ldo.c:148
#9  0x0000000000431188 in lua_resume (L=L@entry=0xf846b8, from=from@entry=0xf7c018,
    nargs=nargs@entry=0x0, nresults=nresults@entry=0x7fff48258f1c) at ldo.c:686
#10 0x0000000000505809 in auxresume (narg=0x0, co=0xf846b8, L=0xf7c018)
```

Sent from Mail for Windows 10

- **Follow-Ups**:
    - **Re: Segmentation fault in changedline**, *Roberto Ierusalimschy*

- Prev by Date: **Re: New param in lua_resume in Lua 5.4**
- Next by Date: **[ANN] lua-bint - Arbitrary precision integer arithmetic library in pure Lua**
- Previous by thread: **lmprof/luajit/torch/threads**
- Next by thread: **Re: Segmentation fault in changedline**
- Index(es):
    - **Date**
    - **Thread**