Freeciv - Bug #688119

Intermittent segfault invoking Lua direction functions

2017-08-03 11:15 PM - Jacob Nevins

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marko Lindqvist	**% Done:**	0%
Category:	Scripting API	**Estimated time:**	0.00 hour
Sprint/Milestone:	2.6.3		

Description

I provoked a segfault twice while mucking around with the new "direction" module added in gna patch #5415.

It doesn't seem 100% reproducible, but it seems to happen sooner or later. I haven't worked out if it's specific to the 'direction' module or a general Lua problem or what; I haven't investigated at all.

The first segfault (for which I didn't get a coredump) was in response to

```
> /lua cmd print(direction.opposite(direction.str2dir("north")))
Segmentation fault (core dumped)
```

This exact command didn't provoke a segfault the second time, but I got one eventually:

```
2: Now accepting new client connections on port 5556.

For introductory help, type 'help'.
> /lua cmd print(direction.opposite(direction.str2dir("north")))
tolua.Direction: 0x233f6a8
> /lua cmd print(direction.str2dir("north"))
tolua.Direction: 0x233fd38
> /lua cmd print(direction.opposite(direction.str2dir("north")))
tolua.Direction: 0x233f6e8
> /lua cmd print(direction.opposite(direction.str2dir("north")))
tolua.Direction: 0x2340818
> /lua cmd print(direction.opposite(direction.str2dir("north")))
tolua.Direction: 0x2340228
> /lua cmd print(direction.opposite(direction.str2dir("east")))
tolua.Direction: 0x2341468
> /lua cmd print(direction.opposite(direction.str2dir("west")))
tolua.Direction: 0x2341938
>
>
> /lua cmd print(direction.opposite(direction.str2dir("south")))
tolua.Direction: 0x2341e58
> /lua cmd print(direction.opposite(direction.str2dir("southwest")))
tolua.Direction: 0x2342088
> /lua cmd print(direction.cw(direction.str2dir("southwest")))
Segmentation fault (core dumped)

#0  0x0000000000000000 in ?? ()
No symbol table info available.
#1  0x0000000000486a5f in luaD_precall (L=L@entry=0x31cebd8, func=0x233f7d0, nresults=0) at /home/
jtn/src/freeciv/git26/dependencies/lua-5.3/src/ldo.c:434
        n = <optimised out>
        f = 0x0
        ci = 0x31e1370
        __PRETTY_FUNCTION__ = "luaD_precall"
#2  0x0000000000486db0 in luaD_call (L=L@entry=0x31cebd8, func=<optimised out>, nResults=nResults@
entry=0) at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/ldo.c:498
No locals.
#3  0x0000000000486e1e in luaD_callnoyield (L=L@entry=0x31cebd8, func=<optimised out>, nResults=nR
esults@entry=0) at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/ldo.c:509
No locals.
```

```
#4  0x0000000000481b58 in lua_callk (L=L@entry=0x31cebd8, nargs=nargs@entry=1, nresults=nresults@e
ntry=0, ctx=ctx@entry=0, k=k@entry=0x0) at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/la
pi.c:924
        func = <optimised out>
        __PRETTY_FUNCTION__ = "lua_callk"
#5  0x000000000051dd21 in class_gc_event (L=0x31cebd8) at /home/jtn/src/freeciv/git26/dependencies
/tolua-5.2/src/lib/tolua_event.c:392
        top = 1
        u = 0x2341cc0
        L = 0x31cebd8
#6  0x0000000000486a5f in luaD_precall (L=L@entry=0x31cebd8, func=0x233f7a0, nresults=0) at /home/
jtn/src/freeciv/git26/dependencies/lua-5.3/src/ldo.c:434
        n = <optimised out>
        f = 0x51dbe0 <class_gc_event>
        ci = 0x31f9570
        __PRETTY_FUNCTION__ = "luaD_precall"
#7  0x0000000000486db0 in luaD_call (L=L@entry=0x31cebd8, func=<optimised out>, nResults=<optimise
d out>) at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/ldo.c:498
No locals.
#8  0x0000000000486e1e in luaD_callnoyield (L=0x31cebd8, func=<optimised out>, nResults=<optimised
 out>) at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/ldo.c:509
No locals.
#9  0x00000000004860d7 in luaD_rawrunprotected (L=L@entry=0x31cebd8, f=f@entry=0x488480 <dothecall
>, ud=ud@entry=0x0) at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/ldo.c:142
        oldnCcalls = 0
        lj = {previous = 0x7ffd21f237d0, b = {{__jmpbuf = {52227032, -8116456252834924501, 0, 2, 0
, 52227128, -8116456252801370069, 8117401323170609195}, __mask_was_saved = 0, __saved_mask = {__va
l = {0, 0, 140725172974720, 140020927570148, 1, 52227240, 140725172974720, 0, 40, 40, 140725172974
848, 140020927570148, 52227128, 80, 0, 4752512}}}}, status = 0}
#10 0x00000000004871d4 in luaD_pcall (L=L@entry=0x31cebd8, func=func@entry=0x488480 <dothecall>, u
=u@entry=0x0, old_top=80, ef=ef@entry=0) at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/l
do.c:729
        status = <optimised out>
        old_ci = 0x31cec38
        old_allowhooks = 0 '\000'
        old_nny = 2
        old_errfunc = 0
#11 0x0000000000488381 in GCTM (L=L@entry=0x31cebd8, propagateerrors=propagateerrors@entry=1) at /
home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/lgc.c:822
        status = <optimised out>
        oldah = 1 '\001'
        running = 1
        g = 0x31ceca8
        tm = <optimised out>
        v = {value_ = {gc = 0x2342060, p = 0x2342060, b = 36970592, f = 0x2342060, i = 36970592, n
 = 1.8265899413613223e-316}, tt_ = 71}
#12 0x0000000000488444 in runafewfinalizers (L=L@entry=0x31cebd8) at /home/jtn/src/freeciv/git26/d
ependencies/lua-5.3/src/lgc.c:848
        g = 0x31ceca8
        i = 0
#13 0x0000000000489be6 in luaC_step (L=L@entry=0x31cebd8) at /home/jtn/src/freeciv/git26/dependenc
ies/lua-5.3/src/lgc.c:1144
        g = <optimised out>
        debt = <optimised out>
#14 0x000000000051c71d in luaX_newstring (ls=ls@entry=0x7ffd21f236d0, str=<optimised out>, l=<opti
mised out>) at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/llex.c:137
        L = 0x31cebd8
        o = <optimised out>
        ts = 0x31cf6c0
#15 0x000000000051d149 in llex (ls=ls@entry=0x7ffd21f236d0, seminfo=seminfo@entry=0x7ffd21f236e8)
at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/llex.c:529
        ts = <optimised out>
#16 0x000000000051d5b9 in luaX_next (ls=ls@entry=0x7ffd21f236d0) at /home/jtn/src/freeciv/git26/de
pendencies/lua-5.3/src/llex.c:556
No locals.
#17 0x000000000048dfee in mainfunc (fs=0x7ffd21f23690, ls=0x7ffd21f236d0) at /home/jtn/src/freeciv
/git26/dependencies/lua-5.3/src/lparser.c:1619
```

```
        bl = {previous = 0x0, firstlabel = 0, firstgoto = 0, nactvar = 0 '\000', upval = 0 '\000',
 isloop = 0 '\000'}
        v = {k = VLOCAL, u = {ival = 0, nval = 0, info = 0, ind = {idx = 0, t = 0 '\000', vt = 0 '
\000'}}, t = -1, f = -1}
#18 luaY_parser (L=L@entry=0x31cebd8, z=0x7ffd21f23990, buff=buff@entry=0x7ffd21f23918, dyd=dyd@en
try=0x7ffd21f23930, name=0x6a9d76 "cmd", firstchar=firstchar@entry=112) at /home/jtn/src/freeciv/g
it26/dependencies/lua-5.3/src/lparser.c:1643
        lexstate = {current = 40, linenumber = 1, lastline = 1, t = {token = 0, seminfo = {r = 0,
i = 0, ts = 0x0}}, lookahead = {token = 289, seminfo = {r = 6.9179530011235576e-310, i = 140020927
570148, ts = 0x7f5929a620e4 <mcount+52>}}, fs = 0x7ffd21f23690, L = 0x31cebd8, z = 0x7ffd21f23990,
 buff = 0x7ffd21f23918, h = 0x2340d40, dyd = 0x7ffd21f23930, source = 0x2337cd0, envn = 0x31f7df0}
        funcstate = {f = 0x2340d80, prev = 0x0, ls = 0x7ffd21f236d0, bl = 0x7ffd21f23650, pc = 0,
lasttarget = 0, jpc = -1, nk = 0, np = 0, firstlocal = 0, nlocvars = 0, nactvar = 0 '\000', nups =
 1 '\001', freereg = 0 '\000'}
        cl = 0x2340d10
#19 0x000000000048600b in f_parser (L=L@entry=0x31cebd8, ud=ud@entry=0x7ffd21f23910) at /home/jtn/
src/freeciv/git26/dependencies/lua-5.3/src/ldo.c:776
        cl = <optimised out>
        p = 0x7ffd21f23910
        c = 112
#20 0x00000000004860d7 in luaD_rawrunprotected (L=L@entry=0x31cebd8, f=f@entry=0x485fa0 <f_parser>
, ud=ud@entry=0x7ffd21f23910) at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/ldo.c:142
        oldnCcalls = 0
        lj = {previous = 0x0, b = {{__jmpbuf = {52227032, -8116456252969142229, 0, 2, 1, 52227128,
 -8116456252935587797, 8117401323170609195}, __mask_was_saved = 0, __saved_mask = {__val = {140725
172976032, 4717488, 140020228816896, 52227032, 0, 52227032, 10330287820725729323, 0, 1, 1, 1407251
72975872, 140020927570148, 7119388, 32, 140725172975888, 4743072}}}}, status = 0}
#21 0x00000000004871d4 in luaD_pcall (L=L@entry=0x31cebd8, func=func@entry=0x485fa0 <f_parser>, u=
u@entry=0x7ffd21f23910, old_top=32, ef=<optimised out>) at /home/jtn/src/freeciv/git26/dependencie
s/lua-5.3/src/ldo.c:729
        status = <optimised out>
        old_ci = 0x31cec38
        old_allowhooks = 1 '\001'
        old_nny = 2
        old_errfunc = 0
#22 0x00000000004872c1 in luaD_protectedparser (L=L@entry=0x31cebd8, z=z@entry=0x7ffd21f23990, nam
e=name@entry=0x6a9d76 "cmd", mode=mode@entry=0x0) at /home/jtn/src/freeciv/git26/dependencies/lua-
5.3/src/ldo.c:793
        p = {z = 0x7ffd21f23990, buff = {buffer = 0x2340e00 "print\177", n = 5, buffsize = 32}, dy
d = {actvar = {arr = 0x0, n = 0, size = 0}, gt = {arr = 0x0, n = 0, size = 0}, label = {arr = 0x0,
 n = 0, size = 0}}, mode = 0x0, name = 0x6a9d76 "cmd"}
        status = <optimised out>
#23 0x0000000000481e88 in lua_load (L=L@entry=0x31cebd8, reader=reader@entry=0x482780 <getS>, data
=data@entry=0x7ffd21f239f0, chunkname=chunkname@entry=0x6a9d76 "cmd", mode=mode@entry=0x0) at /hom
e/jtn/src/freeciv/git26/dependencies/lua-5.3/src/lapi.c:998
        z = {n = 45, p = 0x7ffd21f263da "direction.cw(direction.str2dir(\"southwest\")))", reader
= 0x482780 <getS>, data = 0x7ffd21f239f0, L = 0x31cebd8}
        status = <optimised out>
#24 0x0000000000483d43 in luaL_loadbufferx (L=L@entry=0x31cebd8, buff=buff@entry=0x7ffd21f263d4 "p
rint(direction.cw(direction.str2dir(\"southwest\")))", size=<optimised out>, name=name@entry=0x6a9
d76 "cmd", mode=mode@entry=0x0) at /home/jtn/src/freeciv/git26/dependencies/lua-5.3/src/lauxlib.c:
760
        ls = {s = 0x7ffd21f263d4 "print(direction.cw(direction.str2dir(\"southwest\")))", size = 0
}
#25 0x0000000000688c96 in luascript_do_string (fcl=0x31ceb90, str=str@entry=0x7ffd21f263d4 "print(
direction.cw(direction.str2dir(\"southwest\")))", name=name@entry=0x6a9d76 "cmd") at /home/jtn/src
/freeciv/git26/common/scriptcore/luascript.c:551
        status = <optimised out>
        __FUNCTION__ = "luascript_do_string"
#26 0x000000000047c8f4 in script_server_do_string (caller=caller@entry=0x0, str=str@entry=0x7ffd21
f263d4 "print(direction.cw(direction.str2dir(\"southwest\")))") at /home/jtn/src/freeciv/git26/ser
ver/scripting/script_server.c:96
        status = <optimised out>
        save_caller = 0x0
        save_output_fct = 0x0
#27 0x0000000000448cdb in lua_command (caller=caller@entry=0x0, arg=arg@entry=0x7ffd21f263d0 "cmd
print(direction.cw(direction.str2dir(\"southwest\")))", check=check@entry=false) at /home/jtn/src/
```

```
freeciv/git26/server/stdinhand.c:4746
        script_file = <optimised out>
        extension = ".lua"
        real_filename = 0x0
        luafile = '\000' <repeats 712 times>...
        tilde_filename = '\000' <repeats 888 times>...
        tokens = {0x23421b0 "cmd"}
        luaarg = 0x7ffd21f263d4 "print(direction.cw(direction.str2dir(\"southwest\")))"
        ntokens = 1
        ind = 0
        result = <optimised out>
        ret = false
#28 0x000000000044f383 in handle_stdin_input_real (caller=caller@entry=0x0, str=<optimised out>, s
tr@entry=0x2340cc0 "/lua cmd print(direction.cw(direction.str2dir(\"southwest\")))", check=check@e
ntry=false, read_recursion=read_recursion@entry=0) at /home/jtn/src/freeciv/git26/server/stdinhand
.c:4366
        full_command = "lua cmd print(direction.cw(direction.str2dir(\"southwest\")))\000t\")))\00
0\362!\375\177\000\000\330\353\034\003\000\000\000\000\240^\362!\375\177\000\000@\000\000\000\000\
000\000\000\314\067\060\002\000\000\000\000$\200\200\001\000\000\000\000\317\000\000\000\000\000\0
00\000\270H0\002\000\000\000\000\240\\\362!\375\177\000\000\344 \246)Y\177\000\000 \000\000\000\00
0\000\000\000\317\000\000\000\000\000\000\000!\000\000\000\000\000\000\000\317\000\000\000\000\000
\000\000\001\000\000\000\375\177\000\000\240\000\000\000\000\000\000\000\317\000\000\000\317\000\0
00\000"...
        command = "lua\000\000\000\000\000n\000\000\000w", '\000' <repeats 11 times>, "\017`\362!\3
75\177\000\000\200\t\226)Y\177\000\000\367\236\362!\375\177\000\000|\000\000\000\375\177\000\000\00
0\000\000\000\000\000\000\000\300\353\061\002\000\000\000\000\342\354\061\002\000\000\000\000,a\362
!\375\177\000\000\375)Y\177\000\000\000\000\000\000\000\000\000\000`7\322)Y\177\000\000\n\000\000\
000\000\000\000\000\000\001\000\000\000\000\000\000\000\002\000\000\000\000\000\000\000\342\354\061\00
2\000\000\000\000,a\362!\375\177\000\000\340:\236)Y\177\000\000\342\354\061\002\000\000\000\000\24
0\354\061\002\000\000\000\000P \b\004\000\000\000\000\200\t\226)Y\177\000\000\002\000\000\000\000\
000\000\000\320"...
        arg = "cmd print(direction.cw(direction.str2dir(\"southwest\")))\000t\")))", '\000' <repea
ts 19 times>, "\004", '\000' <repeats 15 times>, "\060f\362!\375\177\000\000\060\036\b\004\000\000
\000\000\300\036\b\004\000\000\000\000\200d\362!\375\177\000\000pd\362!\375\177\000\000\310\035\b\
004\000\000\000\000\220d\362!\375\177\000\000\240d\362!\375\177\000\000\000\000\000\000\000\000\00
0\000\a", '\000' <repeats 15 times>, "u\000\000\000w\000\000\000,\353\061\002\000\000\000\000"...
        cptr_s = <optimised out>
        cptr_d = <optimised out>
        cmd = CMD_LUA
        level = <optimised out>
        __FUNCTION__ = "handle_stdin_input_real"
#29 0x0000000000451c03 in handle_stdin_input (caller=caller@entry=0x0, str=str@entry=0x2340cc0 "/l
ua cmd print(direction.cw(direction.str2dir(\"southwest\")))") at /home/jtn/src/freeciv/git26/serv
er/stdinhand.c:4102
No locals.
#30 0x000000000050179c in handle_readline_input_callback (line=0x2341670 "/lua cmd print(direction
.cw(direction.str2dir(\"southwest\")))") at /home/jtn/src/freeciv/git26/server/sernet.c:189
        line_internal = 0x2340cc0 "/lua cmd print(direction.cw(direction.str2dir(\"southwest\")))"

        line = 0x2341670 "/lua cmd print(direction.cw(direction.str2dir(\"southwest\")))"
#31 0x00007f592b62b63e in rl_callback_read_char () from /lib/x86_64-linux-gnu/libreadline.so.6
No symbol table info available.
#32 0x00000000005035e9 in server_sniff_all_input () at /home/jtn/src/freeciv/git26/server/sernet.c
:798
        i = <optimised out>
        s = <optimised out>
        max_desc = <optimised out>
        readfs = {fds_bits = {1, 0 <repeats 15 times>}}
        writefs = {fds_bits = {0 <repeats 16 times>}}
        exceptfs = {fds_bits = {0 <repeats 16 times>}}
        tv = {tv_sec = 0, tv_usec = 826276}
        __FUNCTION__ = "server_sniff_all_input"
#33 0x000000000043f32a in srv_main () at /home/jtn/src/freeciv/git26/server/srv_main.c:3273
        __FUNCTION__ = "srv_main"
#34 0x00000000004351da in main (argc=1, argv=0x7ffd21f285c8) at /home/jtn/src/freeciv/git26/server
/civserver.c:476
        inx = 1
```

```
        showhelp = <optimised out>
        showvers = <optimised out>
        option = <optimised out>
        __FUNCTION__ = "main"
```

Related issues:

Related to Freeciv - Feature #657148: Lua handling of cardinal directions	**New**
Is duplicate of Freeciv - Bug #880869: Some bug with tolua-5.2 garbage collec...	**Closed**

History

#1 - 2017-08-05 10:12 AM - Jacob Nevins

I've provoked trouble on the S2_5 branch (commit:6fda16cd21) as well.

I still have investigated it adequately, but some observations:

- The number (pointer?) that's printed is different every time, but ought to represent the same direction?
- "Direction" is the only one of the Lua classes which is backed by an enum; all the others are structs.

```
For introductory help, type 'help'.
> /lua cmd print(str2direction("northeast"))
userdata: 0x2229738
> /lua cmd print(str2direction("northeast"))
userdata: 0x22310f8
> /lua cmd print(str2direction("northeast"))
userdata: 0x22318a8
> /lua cmd print(str2direction("northeast"))
userdata: 0x2231c48
> /lua cmd print(str2direction("northeast"))
userdata: 0x22317f8
> /lua cmd print(str2direction("northeast"))
userdata: 0x2232588
> /lua cmd print(str2direction("northeast"))
userdata: 0x2232988
> /lua cmd print(str2direction("northeast"))
userdata: 0x2232d88
> /lua cmd print(str2direction("northeast"))
userdata: 0x2233558
> /lua cmd print(str2direction("northeast"))
userdata: 0x2233638
> /lua cmd print(str2direction("northeast"))
userdata: 0x221cfe8
> /lua cmd print(str2direction("northeast"))
Segmentation fault (core dumped)

#0  0x0000000000000000 in ?? ()
No symbol table info available.
#1  0x000000000047f31f in luaD_precall (L=L@entry=0x18b55b0, func=<optimised out>, nresults=0) at /home/jtn/sr
c/freeciv/git25/dependencies/lua-5.2/src/ldo.c:319
        f = 0x0
        ci = <optimised out>
        n = <optimised out>
        funcr = <optimised out>
        __PRETTY_FUNCTION__ = "luaD_precall"
#2  0x000000000047f775 in luaD_call (L=L@entry=0x18b55b0, func=<optimised out>, nResults=nResults@entry=0, all
owyield=allowyield@entry=0) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/ldo.c:401
No locals.
#3  0x000000000047ad77 in lua_callk (L=L@entry=0x18b55b0, nargs=nargs@entry=1, nresults=nresults@entry=0, ctx=
ctx@entry=0, k=k@entry=0x0) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/lapi.c:905
        func = <optimised out>
        __PRETTY_FUNCTION__ = "lua_callk"
#4  0x0000000000507c61 in class_gc_event (L=0x18b55b0) at /home/jtn/src/freeciv/git25/dependencies/tolua-5.2/s
rc/lib/tolua_event.c:368
        top = 1
        u = 0x221ce60
        L = 0x18b55b0
#5  0x000000000047f31f in luaD_precall (L=L@entry=0x18b55b0, func=<optimised out>, nresults=0) at /home/jtn/sr
c/freeciv/git25/dependencies/lua-5.2/src/ldo.c:319
        f = 0x507b20 <class_gc_event>
        ci = <optimised out>
        n = <optimised out>
        funcr = <optimised out>
        __PRETTY_FUNCTION__ = "luaD_precall"
#6  0x000000000047f775 in luaD_call (L=0x18b55b0, func=<optimised out>, nResults=<optimised out>, allowyield=0
```

) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/ldo.c:401
No locals.
#7 0x0000000000047ec54 in luaD_rawrunprotected (L=L@entry=0x18b55b0, f=f@entry=0x480cb0 <dothecall>, ud=ud@entry=0x0) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/ldo.c:131
        oldnCcalls = 0
        lj = {previous = 0x7fff0be48e40, b = {{__jmpbuf = {25908656, -5026638133634038483, 0, 2, 0, 25908784, -5026638133667592915, 5027104021865661741}, __mask_was_saved = 0, __saved_mask = {__val = {44, 4701477, 140733392915152, 4728647, 140733392915232, 140613907198180, 24106496, 2, 18446744073709551613, 24109888, 140733392915280, 140613907198180, 37308448, 80, 0, 4721840}}}}, status = 0}
#8 0x0000000000047fa58 in luaD_pcall (L=L@entry=0x18b55b0, func=func@entry=0x480cb0 <dothecall>, u=u@entry=0x0, old_top=80, ef=ef@entry=0) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/ldo.c:603
        status = <optimised out>
        old_ci = 0x18b5630
        old_allowhooks = 0 '\000'
        old_nny = 2
        old_errfunc = 0
#9 0x0000000000480bf4 in GCTM (L=L@entry=0x18b55b0, propagateerrors=propagateerrors@entry=1) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/lgc.c:824
        status = <optimised out>
        oldah = 1 '\001'
        running = 1
        g = 0x18b5680
        tm = <optimised out>
        v = {value_ = {gc = 0x221cfc0, p = 0x221cfc0, b = 35770304, f = 0x221cfc0, n = 1.7672878347697725e-316}, tt_ = 71}
#10 0x00000000004825e1 in luaC_forcestep (L=0x18b55b0) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/lgc.c:1170
        g = 0x18b5680
        i = <optimised out>
#11 0x00000000004826ee in luaC_step (L=L@entry=0x18b55b0) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/lgc.c:1179
        g = <optimised out>
#12 0x0000000000506711 in luaX_newstring (ls=ls@entry=0x7fff0be48d40, str=<optimised out>, l=<optimised out>) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/llex.c:134
        L = 0x18b55b0
        o = <optimised out>
        ts = 0x2216a70
#13 0x0000000000507239 in llex (ls=ls@entry=0x7fff0be48d40, seminfo=seminfo@entry=0x7fff0be48d58) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/llex.c:494
        ts = <optimised out>
#14 0x00000000005075f9 in luaX_next (ls=ls@entry=0x7fff0be48d40) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/llex.c:521
No locals.
#15 0x0000000000486521 in mainfunc (fs=0x7fff0be48cf0, ls=0x7fff0be48d40) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/lparser.c:1611
        bl = {previous = 0x0, firstlabel = 0, firstgoto = 0, nactvar = 0 '\000', upval = 0 '\000', isloop = 0 '\000'}
        v = {k = VLOCAL, u = {ind = {idx = 0, t = 0 '\000', vt = 0 '\000'}, info = 0, nval = 0}, t = -1, f = -1}
#16 luaY_parser (L=L@entry=0x18b55b0, z=0x7fff0be49000, buff=buff@entry=0x7fff0be48f88, dyd=dyd@entry=0x7fff0be48fa0, name=0x6929cd "cmd", firstchar=firstchar@entry=112) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/lparser.c:1632
        lexstate = {current = 40, linenumber = 1, lastline = 1, t = {token = 3, seminfo = {r = 1.8432822456454563e-316, ts = 0x2394820}}, lookahead = {token = 286, seminfo = {r = 6.94725008741299 08e-310, ts = 0x7fe339fd30e4 <mcount+52>}}, fs = 0x7fff0be48cf0, L = 0x18b55b0, z = 0x7fff0be49000, buff = 0x7fff0be48f88, dyd = 0x7fff0be48fa0, source = 0x2229650, envn = 0x2242a70, decpoint = 46 '.'}
        funcstate = {f = 0x221d070, h = 0x221d130, prev = 0x0, ls = 0x7fff0be48d40, bl = 0x7fff0be48cc0, pc = 0, lasttarget = 0, jpc = -1, nk = 0, np = 0, firstlocal = 0, nlocvars = 0, nactvar = 0 '\000', nups = 1 '\001', freereg = 0 '\000'}
        cl = 0x221d040
#17 0x0000000000047eb33 in f_parser (L=L@entry=0x18b55b0, ud=ud@entry=0x7fff0be48f80) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/ldo.c:651
        i = <optimised out>
        cl = <optimised out>
        p = 0x7fff0be48f80
        c = 112
#18 0x0000000000047ec54 in luaD_rawrunprotected (L=L@entry=0x18b55b0, f=f@entry=0x47eac0 <f_parser>, ud=ud@entry=0x7fff0be48f80) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/ldo.c:131
        oldnCcalls = 0
        lj = {previous = 0x0, b = {{__jmpbuf = {25908656, -5026638133772450515, 0, 2, 1, 25908784, -5026638133806004947, 5027104021865661741}, __mask_was_saved = 0, __saved_mask = {__val = {140733392916384, 4713556, 140733392916496, 4689424, 0, 25908656, 0, 25908656, 13420105939953878317, 0, 140733392916336, 140613907198180, 7016479, 32, 140733392916352, 4713152}}}}, status = 0}
#19 0x0000000000047fa58 in luaD_pcall (L=L@entry=0x18b55b0, func=func@entry=0x47eac0 <f_parser>, u=u@entry=0x7fff0be48f80, old_top=32, ef=<optimised out>) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/ldo.c:603

```
        status = <optimised out>
        old_ci = 0x18b5630
        old_allowhooks = 1 '\001'
        old_nny = 2
        old_errfunc = 0
#20 0x000000000047fb3b in luaD_protectedparser (L=L@entry=0x18b55b0, z=z@entry=0x7fff0be49000, name=name@entry
=0x6929cd "cmd", mode=mode@entry=0x0) at /home/jtn/src/freeciv/git25/dependencies/lua-5.2/src/ldo.c:672
        p = {z = 0x7fff0be49000, buff = {buffer = 0x221d100 "print\177", n = 5, buffsize = 32}, dyd = {actvar
= {arr = 0x0, n = 0, size = 0}, gt = {arr = 0x0, n = 0, size = 0}, label = {arr = 0x0, n = 0, size = 0}}, mode
 = 0x0, name = 0x6929cd "cmd"}
        status = <optimised out>
#21 0x000000000047b0a8 in lua_load (L=L@entry=0x18b55b0, reader=reader@entry=0x47b970 <getS>, data=data@entry=
0x7fff0be49060, chunkname=chunkname@entry=0x6929cd "cmd", mode=mode@entry=0x0) at /home/jtn/src/freeciv/git25/
dependencies/lua-5.2/src/lapi.c:980
        z = {n = 27, p = 0x7fff0be4bb1a "str2direction(\"northeast\"))", reader = 0x47b970 <getS>, data = 0x7f
ff0be49060, L = 0x18b55b0}
        status = <optimised out>
#22 0x000000000047d193 in luaL_loadbufferx (L=L@entry=0x18b55b0, buff=buff@entry=0x7fff0be4bb14 "print(str2dir
ection(\"northeast\"))", size=<optimised out>, name=name@entry=0x6929cd "cmd", mode=mode@entry=0x0) at /home/j
tn/src/freeciv/git25/dependencies/lua-5.2/src/lauxlib.c:687
        ls = {s = 0x7fff0be4bb14 "print(str2direction(\"northeast\"))", size = 0}
#23 0x00000000006763a6 in luascript_do_string (fcl=0x21fb8e0, str=str@entry=0x7fff0be4bb14 "print(str2directio
n(\"northeast\"))", name=name@entry=0x6929cd "cmd") at /home/jtn/src/freeciv/git25/common/scriptcore/luascript
.c:557
        status = <optimised out>
        __FUNCTION__ = "luascript_do_string"
#24 0x0000000000476c44 in script_server_do_string (caller=caller@entry=0x0, str=str@entry=0x7fff0be4bb14 "prin
t(str2direction(\"northeast\"))") at /home/jtn/src/freeciv/git25/server/scripting/script_server.c:96
        status = <optimised out>
        save_caller = 0x0
        save_output_fct = 0x0
#25 0x000000000044352b in lua_command (caller=caller@entry=0x0, arg=arg@entry=0x7fff0be4bb10 "cmd print(str2di
rection(\"northeast\"))", check=check@entry=false) at /home/jtn/src/freeciv/git25/server/stdinhand.c:4749
        script_file = <optimised out>
        extension = ".lua"
        real_filename = 0x0
        luafile = '\000' <repeats 920 times>...
        tilde_filename = '\000' <repeats 1096 times>...
        tokens = {0x221cec0 "cmd"}
        luaarg = 0x7fff0be4bb14 "print(str2direction(\"northeast\"))"
        ntokens = 1
        ind = 0
        result = <optimised out>
        ret = false
#26 0x000000000044a752 in handle_stdin_input_real (caller=caller@entry=0x0, str=<optimised out>, str@entry=0x2
21ce80 "/lua cmd print(str2direction(\"northeast\"))", check=check@entry=false, read_recursion=read_recursion@
entry=0) at /home/jtn/src/freeciv/git25/server/stdinhand.c:4399
        full_command = "lua cmd print(str2direction(\"northeast\"))\000#\002\000\000\000\000\220\263\344\v\377
\177\000\000`G):\343\177\000\000(", '\000' <repeats 15 times>, "(", '\000' <repeats 15 times>, "\n\000\000\000
\000\000\000\000\340J\365\071\343\177\000\000(\000\000\000\000\000\000\000\200V\213\001\000\000\000\000\340\26
3\344\v\377\177\000\000G'H\000\000\000\000\000\020\264\344\v\377\177\000\000\260U\213\001\000\000\000\000\360P
#\002", '\000' <repeats 12 times>, "\n\000\000\000\000\000\000\000\200V\213\001", '\000' <repeats 12 times>...
        command = "lua\000\000\000\000\000n\000\000\000w", '\000' <repeats 11 times>, "O\267\344\v\377\177\000
\000\200\031\355\071\343\177\000\000\367\376\344\v\377\177\000\000|\000\000\000\377\177\000\000\000\000\000\00
0\000\000\000\000\340\065$\002\000\000\000\000\"7$\002\000\000\000\000l\270\344\v\377\177\000\000\375\353\375\
071\343\177\000\000\000\000\000\000\000\000\000\000`G):\343\177\000\000\n\000\000\000\000\000\000\000\001\000\
000\000\000\000\000\000\002\000\000\000\000\000\000\000\"7$\002\000\000\000\000l\270\344\v\377\177\000\000\340
J\365\071\343\177\000\000\"7$\002\000\000\000\000\340\066$\002\000\000\000\000\320\r\023\003\000\000\000\000\2
00\031\355\071\343\177\000\000\002\000\000\000\000\000\000\000\000"...
        arg = "cmd print(str2direction(\"northeast\"))", '\000' <repeats 11 times>, "`\273\344\v\377\177\000\0
00 \v\023\003\000\000\000\000(\274\344\v\377\177\000\000\001\000\000\000\000\000\000\000UTF-8//\000\000\000\00
0\000\000\000\000\000`\274\344\v\377\177\000\000\000\000\000\000\000\000\000\000\310\t\023\003\000\000\000\000
\002\000\000\000\000\000\000\000\060\n\023\003\000\000\000\000\000\020\000\000\000\000\000\000\360\274\344\v\3
77\177\000\000%g\357\071\343\177\000\000`\274\344\v\377\177\000\000 \001\267\000\000\000\000\000`\274\344\v\37
7\177\000\000\020\v\023\003\000\000\000\000\000\020\000\000\000\000\000\000"...
        cptr_s = <optimised out>
        cptr_d = <optimised out>
        cmd = CMD_LUA
        level = <optimised out>
        __FUNCTION__ = "handle_stdin_input_real"
#27 0x000000000044cdd3 in handle_stdin_input (caller=caller@entry=0x0, str=str@entry=0x221ce80 "/lua cmd print
(str2direction(\"northeast\"))") at /home/jtn/src/freeciv/git25/server/stdinhand.c:4138
No locals.
#28 0x00000000004ef0bc in handle_readline_input_callback (line=0x2215790 "/lua cmd print(str2direction(\"north
east\"))") at /home/jtn/src/freeciv/git25/server/sernet.c:195
```

```
        line_internal = 0x221ce80 "/lua cmd print(str2direction(\"northeast\"))"
        line = 0x2215790 "/lua cmd print(str2direction(\"northeast\"))"
#29 0x00007fe33bb9c63e in rl_callback_read_char () from /lib/x86_64-linux-gnu/libreadline.so.6
No symbol table info available.
#30 0x00000000004f0e97 in server_sniff_all_input () at /home/jtn/src/freeciv/git25/server/sernet.c:800
        i = <optimised out>
        s = <optimised out>
        max_desc = <optimised out>
        readfs = {fds_bits = {1, 0 <repeats 15 times>}}
        writefs = {fds_bits = {0 <repeats 16 times>}}
        exceptfs = {fds_bits = {0 <repeats 16 times>}}
        tv = {tv_sec = 0, tv_usec = 940067}
        __FUNCTION__ = "server_sniff_all_input"
#31 0x0000000000043b061 in srv_main () at /home/jtn/src/freeciv/git25/server/srv_main.c:3046
        __FUNCTION__ = "srv_main"
#32 0x0000000000433034 in main (argc=1, argv=0x7fff0be4db08) at /home/jtn/src/freeciv/git25/server/civserver.c
:468
        inx = 1
        showhelp = <optimised out>
        showvers = <optimised out>
        option = <optimised out>
        __FUNCTION__ = "main"
```

#2 - 2017-08-05 10:13 AM - Jacob Nevins

- Sprint/Milestone changed from 2.6.0 to 2.5.9

Setting target as 2.5.9 to indicate it's not a 2.5.8 blocker, but if there's a simple low-risk fix it can go in 2.5.8, of course.

#3 - 2017-08-19 09:40 AM - Jacob Nevins

- Sprint/Milestone changed from 2.5.9 to 2.5.10

#4 - 2018-01-05 11:12 PM - Marko Lindqvist

- Related to Feature #657148: Lua handling of cardinal directions added

#5 - 2018-01-19 12:46 AM - Jacob Nevins

- Sprint/Milestone changed from 2.5.10 to 2.5.11

#6 - 2018-03-04 12:34 AM - Jacob Nevins

- Sprint/Milestone deleted (2.5.11)

#7 - 2019-12-26 09:48 PM - Jacob Nevins

Had another quick look. Still crashy. No real progress, but things I found:

- tolua is indeed malloc'ing a fresh thing every time an API returns a Direction:

  ```
  Direction tolua_ret =  api_utilities_str2dir(L,str);
  void* tolua_obj = tolua_copy(tolua_S,(void*)&tolua_ret,sizeof(Direction));  /* calls malloc() */
  ```

- Equality is shallow:

  ```
  /lua cmd print(direction.str2dir("north") == direction.str2dir("north"))
  false
  ```

  (not very surprising, but not very helpful either)

#8 - 2020-07-12 09:07 AM - Marko Lindqvist

- Related to Bug #880869: Some bug with tolua-5.2 garbage collecting Direction objects added

#9 - 2020-08-02 01:56 PM - Marko Lindqvist

- Related to deleted (Bug #880869: Some bug with tolua-5.2 garbage collecting Direction objects)

#10 - 2020-08-02 01:56 PM - Marko Lindqvist

- Is duplicate of Bug #880869: Some bug with tolua-5.2 garbage collecting Direction objects added

#11 - 2020-08-02 01:57 PM - Marko Lindqvist

- Category set to Scripting API

- Status changed from New to Closed

- Assignee set to Marko Lindqvist

- Sprint/Milestone set to 2.6.3

Fix is in Bug #880869.