libosmocore - Bug #4164

logging vty session crashes host program if telnet connection is killed

08/21/2019 03:26 PM - neels

Status:	Resolved	**Start date:**	08/21/2019
Priority:	Urgent	**Due date:**	
Assignee:	neels	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

Reproduce, by example of osmo-mgw:

```
osmo-mgw

telnet localhost 4243
# logging enable
# logging level lglobal info

killall telnet
```

libosmocore logs closing of VTY sessions on DLGLOBAL.
If the telnet session is already gone, it can of course no longer log to that telnet session.
But the cleanup of a lost telnet session causes logging while that log target is still half cleaned up.

```
20190821172523272 DLGLOBAL NOTICE Available via telnet 127.0.0.2 4243 (telnet_interface.c:104)
20190821172523273 DLMGCP NOTICE Configured for MGCP, listen on 127.0.0.1:2427 (mgw_main.c:324)
20190821172526667 DLGLOBAL INFO Accept()ed new telnet connection r=127.0.0.1:49490<->l=127.0.0.2:4
243 (telnet_interface.c:186)
20190821172536172 DLGLOBAL INFO Closing telnet connection r=NULL<->l=NULL (telnet_interface.c:132)
../../../../src/libosmocore/src/vty/buffer.c:164:22: runtime error: member access within null poin
ter of type 'struct buffer'

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff70e1ec3 in buffer_put (b=0x0, p=0x7fffffffc210, size=113) at ../../../../src/libosmocor
e/src/vty/buffer.c:164
164         struct buffer_data *data = b->tail;
(gdb) bt
#0  0x00007ffff70e1ec3 in buffer_put (b=0x0, p=0x7fffffffc210, size=113) at ../../../../src/libosm
ocore/src/vty/buffer.c:164
#1  0x00007ffff7102ed6 in vty_out_va (vty=0x6140000010a0, format=0x7ffff71489a0 "%s", ap=0x7ffffff
fc6b0)
    at ../../../../src/libosmocore/src/vty/vty.c:294
#2  0x00007ffff710313f in vty_out (vty=0x6140000010a0, format=0x7ffff71489a0 "%s") at ../../../../
src/libosmocore/src/vty/vty.c:315
#3  0x00007ffff711d3f7 in _vty_output (tgt=0x6120000012a0, level=3,
    line=0x7fffffffc990 "<0002> ../../../../src/libosmocore/src/vty/telnet_interface.c:132 Closing
 telnet connection r=NULL<->l=NULL\n\033[0;m")
    at ../../../../src/libosmocore/src/vty/logging_vty.c:85
#4  0x00007ffff69eb7d2 in _output (target=0x6120000012a0, subsys=2, level=3,
    file=0x7ffff7147dc0 "../../../../src/libosmocore/src/vty/telnet_interface.c", line=132, cont=0
,
    format=0x7ffff7147ec0 "Closing telnet connection %s\n", ap=0x7fffffffda60) at ../../../src/lib
osmocore/src/logging.c:460
#5  0x00007ffff69ec221 in osmo_vlogp (subsys=2, level=3, file=0x7ffff7147dc0 "../../../../src/libo
smocore/src/vty/telnet_interface.c", line=132,
    cont=0, format=0x7ffff7147ec0 "Closing telnet connection %s\n", ap=0x7fffffffdb20) at ../../..
/src/libosmocore/src/logging.c:548
#6  0x00007ffff69ec655 in logp2 (subsys=-1, level=3, file=0x7ffff7147dc0 "../../../../src/libosmoc
ore/src/vty/telnet_interface.c", line=132, cont=0,
    format=0x7ffff7147ec0 "Closing telnet connection %s\n") at ../../../src/libosmocore/src/loggin
g.c:581
```

```
#7  0x00007ffff711b9cf in telnet_close_client (fd=0x6100000014b8) at ../../../../src/libosmocore/src/vty/telnet_interface.c:131
#8  0x00007ffff711d114 in vty_event (event=VTY_CLOSED, sock=-1, vty=0x6140000010a0) at ../../../../src/libosmocore/src/vty/telnet_interface.c:251
#9  0x00007ffff7102a6b in vty_close (vty=0x6140000010a0) at ../../../../src/libosmocore/src/vty/vty.c:240
#10 0x00007ffff71120e7 in vty_read (vty=0x6140000010a0) at ../../../../src/libosmocore/src/vty/vty.c:1449
#11 0x00007ffff711beb3 in client_data (fd=0x6100000014b8, what=1) at ../../../../src/libosmocore/src/vty/telnet_interface.c:154
#12 0x00007ffff69b6871 in osmo_fd_disp_fds (_rset=0x7fffffffe250, _wset=0x7fffffffe2f0, _eset=0x7fffffffe390)
    at ../../../src/libosmocore/src/select.c:223
#13 0x00007ffff69b6b88 in osmo_select_main (polling=0) at ../../../src/libosmocore/src/select.c:263
#14 0x000055555561e8eb in main (argc=3, argv=0x7fffffffe5a8) at ../../../../src/osmo-mgw/src/osmo-mgw/mgw_main.c:339
```

History

#1 - 08/21/2019 03:49 PM - neels

- Assignee set to neels

- % Done changed from 0 to 90

https://gerrit.osmocom.org/c/libosmocore/+/15265

#2 - 08/29/2019 10:10 PM - neels

Actually a 'killall telnet' is not even needed. The exit code path is identical to a normal close, this suffices to trigger the bug:

```
> logging enable
> logging level lglobal info
> exit
```

in any osmocom application

#3 - 08/29/2019 10:53 PM - neels

https://gerrit.osmocom.org/c/libosmocore/+/15339 <-- newer fix

#4 - 09/02/2019 11:05 PM - neels

- Status changed from New to Resolved

- % Done changed from 90 to 100