libosmo-netif - Bug #3685

heap use after free in osmo_stream_srv_write()

11/09/2018 01:27 PM - stsp

Status:	Resolved	**Start date:**	11/09/2018
Priority:	Normal	**Due date:**	
Assignee:	stsp	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

Running the TTCN3 MSC test suite on binaries with address sanitizer enabled, I found this crash in libosmo-netif:

{{{
Fri Nov 9 14:05:02 2018 DLINP <0002> stream.c:849 connected read/write
Fri Nov 9 14:05:02 2018 DLINP <0002> stream.c:789 message received
Fri Nov 9 14:05:02 2018 DLSS7 <000c> osmo_ss7.c:1424 asp-virt-bsc0-0: xua_srv_conn_cb(): sctp_recvmsg() returned 12 (flags=0x8080)
Fri Nov 9 14:05:02 2018 DLSS7 <000c> osmo_ss7.c:1357 asp-virt-bsc0-0: xUA SRV SCTP NOTIFICATION 32773 flags=0x0
Fri Nov 9 14:05:02 2018 DLSS7 <000c> osmo_ss7.c:1370 asp-virt-bsc0-0: xUA SRV SHUTDOWN_EVENT
Fri Nov 9 14:05:02 2018 DLSS7 <000c> osmo_ss7.c:1616 virt-bsc0-0: SCTP connection closed
Fri Nov 9 14:05:02 2018 DLSS7 <000c> osmo_ss7.c:1622 XUA_ASP(virt-bsc0-0){ASP_ACTIVE}: Received Event SCTP-COMM_DOWN.ind
Fri Nov 9 14:05:02 2018 DLSS7 <000c> xua_asp_fsm.c:591 XUA_ASP(virt-bsc0-0){ASP_ACTIVE}: state_chg to ASP_DOWN
Fri Nov 9 14:05:02 2018 DLSS7 <000c> xua_asp_fsm.c:404 XUA_AS(virt-bsc0){AS_ACTIVE}: Received Event ASPAS-ASP_DOWN.ind
Fri Nov 9 14:05:02 2018 DLSS7 <000c> xua_as_fsm.c:263 XUA_AS(virt-bsc0){AS_ACTIVE}: state_chg to AS_PENDING
Fri Nov 9 14:05:02 2018 DLSS7 <000c> xua_asp_fsm.c:125 asp-virt-bsc0-0: No Layer Manager, dropping M-ASP_DOWN.indication
Fri Nov 9 14:05:02 2018 DLSS7 <000c> xua_asp_fsm.c:125 asp-virt-bsc0-0: No Layer Manager, dropping M-SCTP_RELEASE.indication
Fri Nov 9 14:05:02 2018 DLINP <0002> stream.c:811 sending data
===
28165ERROR: AddressSanitizer: heap-use-after-free on address 0x611000007298 at pc 0x7ffff3d20f2f bp 0x7fffffffd6d0 sp 0x7fffffffd6c0
READ of size 8 at 0x611000007298 thread T0
#0 0x7ffff3d20f2e in llist_empty /home/stsp/osmo/prefix/include/osmocom/core/linuxlist.h:167
#1 0x7ffff3d25b17 in osmo_stream_srv_write /home/stsp/osmo/libosmo-netif/src/stream.c:813
#2 0x7ffff3d26312 in osmo_stream_srv_cb /home/stsp/osmo/libosmo-netif/src/stream.c:853
#3 0x7ffff61c0843 in osmo_fd_disp_fds /home/stsp/osmo/libosmocore/src/select.c:217
#4 0x7ffff61c0b44 in osmo_select_main /home/stsp/osmo/libosmocore/src/select.c:257
#5 0x555555556c43 in main /home/stsp/osmo/libosmo-sccp/stp/stp_main.c:210
#6 0x7ffff5038b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#7 0x5555555563e9 in _start (/home/stsp/osmo/prefix/bin/osmo-stp+0x23e9)

0x611000007298 is located 152 bytes inside of 200-byte region [0x611000007200,0x6110000072c8)
freed by thread T0 here:
#0 0x7ffff6ef87b8 in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xde7b8)
#1 0x7ffff6829a52 in _talloc_free (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x3a52)

previously allocated by thread T0 here:
#0 0x7ffff6ef8b50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
#1 0x7ffff682bd20 in _talloc_zero (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x5d20)

SUMMARY: AddressSanitizer: heap-use-after-free /home/stsp/osmo/prefix/include/osmocom/core/linuxlist.h:167 in llist_empty
Shadow bytes around the buggy address:
0x0c227fff8e00: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
0x0c227fff8e10: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x0c227fff8e20: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c227fff8e30: fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c227fff8e40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c227fff8e50: fd fd fd[fd]fd fd fd fd fd fa fa fa fa fa fa fa
0x0c227fff8e60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

```
0x0c227fff8e70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c227fff8e80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c227fff8e90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c227fff8ea0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable:           00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:       fa
Freed heap region:       fd
Stack left redzone:      f1
Stack mid redzone:       f2
Stack right redzone:     f3
Stack after return:      f5
Stack use after scope:   f8
Global redzone:          f9
Global init order:       f6
Poisoned by user:        f7
Container overflow:      fc
Array cookie:            ac
Intra object redzone:    bb
ASan internal:           fe
Left alloca redzone:     ca
Right alloca redzone:    cb
28165ABORTING
}}}
```

History

#1 - 11/09/2018 01:42 PM - stsp

- Subject changed from crash in osmo_stream_srv_write() with address sanitizer to heap use after free in osmo_stream_srv_write()

#2 - 11/09/2018 02:07 PM - stsp

This problem can be fixed with two patches:

return error code from xua_srv_conn_cb() if conn is freed
https://gerrit.osmocom.org/#/c/libosmo-sccp/+/11704

detect freed connections in osmo_stream_srv_read()
https://gerrit.osmocom.org/c/libosmo-netif/+/11705

#3 - 11/09/2018 03:35 PM - stsp

- Status changed from New to Resolved

Above patches have been merged.