OsmoGGSN (former OpenGGSN) - Bug #4641

osmo-ggsn: heap-use-after-free in sgsn_peer_drop_all_pdp_except

07/03/2020 11:38 AM - pespin

Status:	New	**Start date:**	07/03/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

Got it a few seconds after killing (restarting) osmo-sgsn:

```
20200703132046337 DGGSN <0002> /git/osmo-ggsn/ggsn/ggsn.c:653 PDP(901700000015256:5): Packet recei
ved on APN(internet): forwarding to tun tun4
20200703132046348 DTUN <0001> /git/osmo-ggsn/ggsn/ggsn.c:632 TUN(tun4): Received packet for APN(in
ternet)
20200703132047218 DGGSN <0002> /git/osmo-ggsn/ggsn/ggsn.c:653 PDP(901700000015256:5): Packet recei
ved on APN(internet): forwarding to tun tun4
20200703132047230 DTUN <0001> /git/osmo-ggsn/ggsn/ggsn.c:632 TUN(tun4): Received packet for APN(in
ternet)
20200703132048335 DGGSN <0002> /git/osmo-ggsn/ggsn/ggsn.c:653 PDP(901700000015256:5): Packet recei
ved on APN(internet): forwarding to tun tun4
20200703132048346 DTUN <0001> /git/osmo-ggsn/ggsn/ggsn.c:632 TUN(tun4): Received packet for APN(in
ternet)
20200703132049416 DGGSN <0002> /git/osmo-ggsn/ggsn/ggsn.c:653 PDP(901700000015256:5): Packet recei
ved on APN(internet): forwarding to tun tun4
20200703132049427 DTUN <0001> /git/osmo-ggsn/ggsn/ggsn.c:632 TUN(tun4): Received packet for APN(in
ternet)
20200703132050417 DGGSN <0002> /git/osmo-ggsn/ggsn/ggsn.c:653 PDP(901700000015256:5): Packet recei
ved on APN(internet): forwarding to tun tun4
20200703132050429 DTUN <0001> /git/osmo-ggsn/ggsn/ggsn.c:632 TUN(tun4): Received packet for APN(in
ternet)
20200703132051335 DGGSN <0002> /git/osmo-ggsn/ggsn/ggsn.c:653 PDP(901700000015256:5): Packet recei
ved on APN(internet): forwarding to tun tun4
20200703132051347 DTUN <0001> /git/osmo-ggsn/ggsn/ggsn.c:632 TUN(tun4): Received packet for APN(in
ternet)
20200703132051636 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:29 SGSN(127.0.0.1): Tx Echo Request
20200703132051636 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:40 SGSN(127.0.0.1): Rx Echo Response
20200703132052318 DGGSN <0002> /git/osmo-ggsn/ggsn/ggsn.c:653 PDP(901700000015256:5): Packet recei
ved on APN(internet): forwarding to tun tun4
20200703132052330 DTUN <0001> /git/osmo-ggsn/ggsn/ggsn.c:632 TUN(tun4): Received packet for APN(in
ternet)
20200703132053256 DGGSN <0002> /git/osmo-ggsn/ggsn/ggsn.c:653 PDP(901700000015256:5): Packet recei
ved on APN(internet): forwarding to tun tun4
20200703132053268 DTUN <0001> /git/osmo-ggsn/ggsn/ggsn.c:632 TUN(tun4): Received packet for APN(in
ternet)
20200703132151636 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:29 SGSN(127.0.0.1): Tx Echo Request
20200703132151637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:40 SGSN(127.0.0.1): Rx Echo Response
20200703132251637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:29 SGSN(127.0.0.1): Tx Echo Request
20200703132251637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:40 SGSN(127.0.0.1): Rx Echo Response
20200703132351637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:29 SGSN(127.0.0.1): Tx Echo Request
20200703132351637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:40 SGSN(127.0.0.1): Rx Echo Response
20200703132451637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:29 SGSN(127.0.0.1): Tx Echo Request
20200703132451637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:40 SGSN(127.0.0.1): Rx Echo Response
20200703132551637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:29 SGSN(127.0.0.1): Tx Echo Request
20200703132551637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:40 SGSN(127.0.0.1): Rx Echo Response
20200703132651637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:29 SGSN(127.0.0.1): Tx Echo Request
20200703132651638 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:40 SGSN(127.0.0.1): Rx Echo Response
20200703132751637 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:29 SGSN(127.0.0.1): Tx Echo Request
20200703132751638 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:40 SGSN(127.0.0.1): Rx Echo Response
20200703132851638 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:29 SGSN(127.0.0.1): Tx Echo Request
```

```
20200703132851638 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:40 SGSN(127.0.0.1): Rx Echo Response
20200703132851638 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:151 SGSN(127.0.0.1): SGSN recovery (174->175) pdp=(nil), releasing all PDP contexts
20200703132851638 DGGSN <0002> /git/osmo-ggsn/ggsn/ggsn.c:66 PDP(901700000015256:5): Sending DELETE PDP CTX due to shutdown
20200703132851638 DGGSN <0002> /git/osmo-ggsn/ggsn/ggsn.c:354 PDP(901700000015256:5): Deleting PDP context
20200703132851638 DGGSN <0002> /git/osmo-ggsn/ggsn/sgsn.c:21 SGSN(127.0.0.1): Deleting SGSN
20200703132851638 DLGTP <000d> /git/osmo-ggsn/gtp/pdp.c:296 Begin pdp_tiddel tid = 5652510000007109
20200703132851638 DLGTP <000d> /git/osmo-ggsn/gtp/pdp.c:303 End pdp_tiddel: PDP found
=================================================================
==12028==ERROR: AddressSanitizer: heap-use-after-free on address 0x611000005848 at pc 0x5555555da90f bp 0x7fffffffb7f0 sp 0x7fffffffb7e0
READ of size 8 at 0x611000005848 thread T0
    #0 0x5555555da90e in sgsn_peer_drop_all_pdp_except /git/osmo-ggsn/ggsn/sgsn.c:123
    #1 0x5555555db031 in sgsn_peer_handle_recovery /git/osmo-ggsn/ggsn/sgsn.c:157
    #2 0x5555555d6a05 in cb_recovery3 /git/osmo-ggsn/ggsn/ggsn.c:782
    #3 0x7ffff74fc66b in emit_cb_recovery /git/osmo-ggsn/gtp/gtp.c:223
    #4 0x7ffff7508769 in gtp_echo_conf /git/osmo-ggsn/gtp/gtp.c:1134
    #5 0x7ffff752a9e1 in gtp_decaps1c /git/osmo-ggsn/gtp/gtp.c:3154
    #6 0x5555555d661e in ggsn_gtp_fd_cb /git/osmo-ggsn/ggsn/ggsn.c:725
    #7 0x7ffff699ef76 in osmo_fd_disp_fds /git/libosmocore/src/select.c:227
    #8 0x7ffff699f35b in _osmo_select_main /git/libosmocore/src/select.c:265
    #9 0x7ffff699f43a in osmo_select_main /git/libosmocore/src/select.c:274
    #10 0x5555555bb31c in main /git/osmo-ggsn/ggsn/ggsn_main.c:201
    #11 0x7ffff5d3a001 in __libc_start_main (/usr/lib/libc.so.6+0x27001)
    #12 0x5555555bab0d in _start (/build/new/out/bin/osmo-ggsn+0x66b0d)

0x611000005848 is located 136 bytes inside of 240-byte region [0x6110000057c0,0x6110000058b0)
freed by thread T0 here:
    #0 0x7ffff766b0e9 in __interceptor_free /build/gcc/src/gcc/libsanitizer/asan/asan_malloc_linux.cpp:123
    #1 0x7ffff689941b  (/usr/lib/libtalloc.so.2+0x441b)

previously allocated by thread T0 here:
    #0 0x7ffff766b459 in __interceptor_malloc /build/gcc/src/gcc/libsanitizer/asan/asan_malloc_linux.cpp:145
    #1 0x7ffff689bb8c  (/usr/lib/libtalloc.so.2+0x6b8c)

SUMMARY: AddressSanitizer: heap-use-after-free /git/osmo-ggsn/ggsn/sgsn.c:123 in sgsn_peer_drop_all_pdp_except
Shadow bytes around the buggy address:
  0x0c227fff8ab0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c227fff8ac0: fd fd fd fd fd fd fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8ad0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c227fff8ae0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa
  0x0c227fff8af0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c227fff8b00: fd fd fd fd fd fd fd fd fd[fd]fd fd fd fd fd fd
  0x0c227fff8b10: fd fd fd fd fd fd fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8b30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8b50: 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
  Shadow gap:              cc
==12028==ABORTING
[Inferior 1 (process 12028) exited with code 01]
(gdb)
```

History

#1 - 07/03/2020 11:43 AM - pespin

Using osmo-ggsn.git 4e37fb356aafda0b12d8b33daa5057c43fe633f5

Failure line is:

```
llist_for_each_entry_safe(pdp, pdp2, &sgsn->pdp_list, entry) {
```

So it looks like some pdp context is left in the pdp_list after being freed (probably by libgtp?).