OsmoGGSN (former OpenGGSN) - Bug #2843

crash by icmpv6 message

01/19/2018 03:54 PM - msuraev

Status:	Resolved	**Start date:**	01/19/2018
Priority:	Normal	**Due date:**	
Assignee:	pespin	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

The OsmoGGSN crashed while trying to handle imcpv6. Curiously, there's no IPv6 enabled on tun interface:

```
ggsn: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default q
len 500
    link/none
    inet 192.168.7.1/24 brd 192.168.7.255 scope global ggsn
       valid_lft forever preferred_lft forever
```

The interface was configured using systemd-networkd, the osmo-ggsn was running without root priveleges.
I'm unable to attach core file due to size limit (it's 135M).
The output from gdb:

```
<0001> ggsn.c:690 Received packet for APN(internet) from tun ggsn
<0001> ggsn.c:690 Received packet for APN(internet) from tun ggsn
<0002> ggsn.c:542 PDP(001640000005666:5): Processing create PDP context request for APN 'internet'
<0002> ggsn.c:642 PDP(001640000005666:5): Successful PDP Context Creation: APN=internet(internet),
 TEIC=1, IP=192.168.7.2
<000d> gtp.c:2887 recvfrom(fd=6, buffer=7fffffffbf20, len=8196) failed: status = 18446744073709551
615 error = Resource temporarily unavailable
<0002> ggsn.c:719 PDP(001640000005666:5): Packet received on APN(internet): forwarding to tun ggsn
Assert failed member icmpv6.c:197
backtrace() returned 8 addresses
/home/max/source/gsm/osmo-ggsn/ggsn/.libs/osmo-ggsn(+0x831e) [0x55555555c31e]
/usr/lib/x86_64-linux-gnu/libgtp.so.2(gtp_gpdu_ind+0xa2) [0x7ffff77afbb2]
/usr/lib/x86_64-linux-gnu/libgtp.so.2(gtp_decaps1u+0x48e) [0x7ffff77b02be]
/usr/lib/x86_64-linux-gnu/libosmocore.so.9(osmo_select_main+0x21f) [0x7ffff6d00baf]
/home/max/source/gsm/osmo-ggsn/ggsn/.libs/osmo-ggsn(+0x37c7) [0x5555555577c7]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf1) [0x7ffff69381c1]
/home/max/source/gsm/osmo-ggsn/ggsn/.libs/osmo-ggsn(+0x390a) [0x55555555790a]

Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
51      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
```

The backtrace:

```
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
        set = {__val = {0 <repeats 11 times>, 5914256997969341952, 0, 93824994527152, 1, 140737488
338096}}
        pid = <optimized out>
        tid = <optimized out>
#1  0x00007ffff694ff5d in __GI_abort () at abort.c:90
        save_stage = 2
        act = {__sigaction_handler = {sa_handler = 0x555555561d98, sa_sigaction = 0x555555561d98},
 sa_mask = {__val = {197, 0,
              93824994989840, 18446744073709551615, 140737488338720, 140737488338704, 6, 6, 2, 140
737488338732, 140737334248496,
              206158430256, 5914256997969341952, 140737347567712, 140737347567712, 48}}, sa_flags
```

```
= 1434408720, sa_restorer = 0x1}
        sigs = {__val = {32, 0 <repeats 15 times>}}
#2  0x000055555555c323 in handle_router_mcast (gsn=<optimized out>, pdp=0x7ffff79bc060 <pdpa>, own
_ll_addr=<optimized out>,
    pack=<optimized out>, len=<optimized out>) at icmpv6.c:197
        member = <optimized out>
        ip6h = <optimized out>
        ic6h = <optimized out>
        msg = <optimized out>
#3  0x00007ffff77afbb2 in gtp_gpdu_ind (gsn=gsn@entry=0x5555557f5710, version=version@entry=1, pee
r=peer@entry=0x7fffffffbf10,
    fd=fd@entry=7, pack=pack@entry=0x7fffffffbf20, len=len@entry=60) at gtp.c:2743
        hlen = 12
        pdp = 0x7ffff79bc060 <pdpa>
#4  0x00007ffff77b02be in gtp_decaps1u (gsn=0x5555557f5710) at gtp.c:3129
        buffer = "2\377\000\064\000\000\000\001\000\000\000\000`\000\000\000\000\b:\377\376\200\00
0\000\000\000\000\000%c\376\005\002\213\aR\377\002", '\000' <repeats 13 times>, "\002\205\000O\361
\000\000\000\000t\204\000\027\200\200!\020\001\001\000\020\201\006\000\000\000\000\203\006\000\000
\000\000\000\r\000\205\000\004\177\000\000\002\205\000\004\177\000\000\002\206\000\001\000\207\000
\016", '\000' <repeats 14 times>, "\227\000\001\002\230\000\b\000\000\361F\000\005\000\000\232\000
\bSY9`\225y\225\360\000\000\000\000\000\000\000\000\340\306\377\377\377\177", '\000' <repeats 14 t
imes>, "\002\000\000\000\002\000\000\000\000\177\000\000\000\307\377\377\377\177\000\000\001\000\0
00\000\000\000\000\000"...
        peer = {sin_family = 2, sin_port = 26632, sin_addr = {s_addr = 33554559}, sin_zero = "\000
\000\000\000\000\000\000"}
        peerlen = 16
        status = 60
        pheader = 0x7fffffffbf20
        fd = 7
#5  0x00007ffff6d00baf in osmo_fd_disp_fds (_eset=0x7fffffffe090, _wset=0x7fffffffe010, _rset=0x7f
ffffffdf90) at select.c:216
        flags = <optimized out>
        flags = <optimized out>
        ufd = <optimized out>
        tmp = <optimized out>
        exceptset = <optimized out>
        work = <optimized out>
        readset = <optimized out>
        writeset = <optimized out>
#6  osmo_select_main (polling=0) at select.c:256
        readset = {__fds_bits = {0 <repeats 16 times>}}
        writeset = {__fds_bits = {0 <repeats 16 times>}}
        exceptset = {__fds_bits = {0 <repeats 16 times>}}
        rc = <optimized out>
        no_time = {tv_sec = 0, tv_usec = 0}
#7  0x00005555555577c7 in main (argc=3, argv=0x7fffffffe278) at ggsn.c:1015
        ggsn = <optimized out>
        rc = <optimized out>
```

The crash is not reliably reproducible but happens from time to time when using galaxy tab 2. Configs are attached.

Related issues:

Related to OsmoSGSN - Bug #1794: support random IV for GEA (via XID)	**Stalled**	**08/09/2016**

History

#1 - 01/19/2018 04:07 PM - msuraev

Also, the dump running on the ggsn interface got no packets at all.

#2 - 01/19/2018 06:12 PM - msuraev

Link to core file: http://people.osmocom.org/~msuraev/core.15573

#3 - 01/19/2018 07:06 PM - pespin

- Assignee set to pespin

Assigning to me as it is coming from a commit I wrote to add ipv4v6 APN support (osmo-ggsn 2d6a69e69a4b4cb2b8cc63c4810dae44e5a4d8f6).

```
-    struct ippoolm_t *member = pdp->peer;
+    struct ippoolm_t *member;
     const struct ip6_hdr *ip6h = (struct ip6_hdr *)pack;
     const struct icmpv6_hdr *ic6h = (struct icmpv6_hdr *) (pack + sizeof(*ip6h));
     struct msgb *msg;

     OSMO_ASSERT(pdp);
+
+    member = pdp->peer[0];
+    OSMO_ASSERT(member);
+    if (member->addr.len == sizeof(struct in_addr)) /* ipv4v6 context */
+        member = pdp->peer[1];
```

In there I assumed that we only receive ipv6 routing packets ("handle_router_mcast") if we have an ipv6 ctx, which was also the previous assumption. I extended it to look for the ipv6 one in case we have 1 ctx with 2 peers (case of apn type ipv4v6). If the first one is ipv4, then then 2nd one must be the ipv6 one.

The tablet used to generate this crash has the APN configured to be used as IPv4 only, same as the sgsn configured APN ("internet"). So we should really check why can an ipv6 packet appear and be received by the ggsn.

So, my understanding is that before this patch, the code didn't assert but was most probably wrongly assuming it was an ipv6 ctx and using not properly initizalied field later in (if ic6h->type is router solicitation):

```
msg = icmpv6_construct_ra(own_ll_addr, &ip6h->ip6_src, &member->addr.v6);
```

It would be really interesting to get the pcap trace done preferrrably in interface "any", or otherwise in "loopback" (if sgsn and ggsn are in the same PC) or the interface connected against the PCU. This way we can see the packet being sent by the mobile phone and see what's the best fix for it.

PS: I think we may be able to get the causing packet from the core file.

#4 - 01/22/2018 10:48 AM - pespin

This failure in recvfrom immediately before the crash also looks suspicious:

```
<000d> gtp.c:2887 recvfrom(fd=6, buffer=7fffffffbf20, len=8196) failed: status = 18446744073709551615 error =
Resource temporarily unavailable
<0002> ggsn.c:719 PDP(001640000005666:5): Packet received on APN(internet): forwarding to tun ggsn
Assert failed member icmpv6.c:197
```

Could it be that the fail path is buggy and ann uninitialized buffer is passed to the upper stack?

#5 - 01/22/2018 11:28 AM - pespin

- Status changed from New to Feedback

- Assignee changed from pespin to msuraev

Are you sure you were using latest rev of osmo-ggsn in here? Because I see the following line in the log:

```
<000d> gtp.c:2887 recvfrom(fd=6, buffer=7fffffffbf20, len=8196) failed: status = 18446744073709551615 error =
Resource temporarily unavailable
```

And looking at the code the line doesn't match with my file (current master) and according to all recvfrom paths in that file, the message cannot be printed (resource temporarily unavailable == EAGAIN, which is handled before the print).

The crash however doesn't seem to be happening directly after it since from the backtrace it can be seen that len=60 in gtp_gpdu_ind instead of a really big number or a negative number indicating the error. But stuff seems to be really messed up there somehow as I indicated above.

Please re-test with latest master and next time also provide the osmo-ggsn binary together with the core file, plus pcap trace.

#6 - 01/22/2018 03:57 PM - msuraev

- Status changed from Feedback to New

- Assignee changed from msuraev to pespin

Reproduced with latest master (36b940d1fed8d5780bb69ec7de0d170939d4745e):
http://people.osmocom.org/~msuraev/core.24024
http://people.osmocom.org/~msuraev/osmo-ggsn
http://people.osmocom.org/~msuraev/libgtp.so.2
http://people.osmocom.org/~msuraev/rs.pcap.pcapng.gz

#7 - 01/22/2018 04:53 PM - msuraev

- Related to Bug #1794: support random IV for GEA (via XID) added

#8 - 01/25/2018 07:58 PM - pespin

- Status changed from New to In Progress

I already have a patch for this one, I'll test and submit tomorrow morning.

#9 - 01/26/2018 08:53 PM - pespin

- Status changed from In Progress to Resolved

- % Done changed from 0 to 100

Fix merged in osmo-ggsn 7d54ed48e78e9666217865f4586c26c6ec896fe6

#10 - 01/27/2018 05:00 PM - laforge

- Status changed from Resolved to In Progress

- % Done changed from 100 to 90

I just noticed we don't have a ttcn3 test for this yet. Should be super easy to add and helps us to ensure this kind of bug doesn't reappear

#11 - 01/30/2018 04:27 PM - pespin

- Status changed from In Progress to Feedback

TEst checking that scenario submitted to https://gerrit.osmocom.org/#/c/6158/. Once it's merged, we can close this one.

#12 - 01/31/2018 03:20 PM - pespin

- Status changed from Feedback to Resolved

- % Done changed from 90 to 100

Merged, closing.

Files

osmo-ggsn.cfg-nonroot	1.05 KB	01/19/2018	msuraev
ggsn.network	90 Bytes	01/19/2018	msuraev
ggsn.netdev	54 Bytes	01/19/2018	msuraev