author	Xin Long <lucien.xin@gmail.com>	2022-11-04 17:45:16 -0400
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2022-12-02 17:40:59 +0100
commit	2ea600b598dd3e061854dd4dd5b4c815397dfcea (patch)	
tree	b16c116e1176573c0c2ca1866bc5ed70be876c7d	
parent	1f9f346fbb78088bab582c0c9e6d509ae3220fb5 (diff)	
download	linux-2ea600b598dd3e061854dd4dd5b4c815397dfcea.tar.gz	

sctp: clear out_curr if all frag chunks of current msg are pruned

```
[ Upstream commit 2f201ae14ae0f91dbf1cffea7bb1e29e81d4d108 ]

A crash was reported by Zhen Chen:

  list_del corruption, ffffa035ddf01c18->next is NULL
  WARNING: CPU: 1 PID: 250682 at lib/list_debug.c:49 __list_del_entry_valid+0x59/0xe0
  RIP: 0010:__list_del_entry_valid+0x59/0xe0
  Call Trace:
   sctp_sched_dequeue_common+0x17/0x70 [sctp]
   sctp_sched_fcfs_dequeue+0x37/0x50 [sctp]
   sctp_outq_flush_data+0x85/0x360 [sctp]
   sctp_outq_uncork+0x77/0xa0 [sctp]
   sctp_cmd_interpreter.constprop.0+0x164/0x1450 [sctp]
   sctp_side_effects+0x37/0xe0 [sctp]
   sctp_do_sm+0xd0/0x230 [sctp]
   sctp_primitive_SEND+0x2f/0x40 [sctp]
   sctp_sendmsg_to_asoc+0x3fa/0x5c0 [sctp]
   sctp_sendmsg+0x3d5/0x440 [sctp]
   sock_sendmsg+0x5b/0x70

and in sctp_sched_fcfs_dequeue() it dequeued a chunk from stream
out_curr outq while this outq was empty.

Normally stream->out_curr must be set to NULL once all frag chunks of
current msg are dequeued, as we can see in sctp_sched_dequeue_done().
However, in sctp_prsctp_prune_unsent() as it is not a proper dequeue,
sctp_sched_dequeue_done() is not called to do this.

This patch is to fix it by simply setting out_curr to NULL when the
last frag chunk of current msg is dequeued from out_curr stream in
sctp_prsctp_prune_unsent().

Fixes: 5bbbbe32a431 ("sctp: introduce stream scheduler foundations")
Reported-by: Zhen Chen <chenzhen126@huawei.com>
Tested-by: Caowangbao <caowangbao@huawei.com>
Signed-off-by: Xin Long <lucien.xin@gmail.com>
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
Signed-off-by: Sasha Levin <sashal@kernel.org>
```

Diffstat

-rw-r--r-- net/sctp/outqueue.c 5

1 files changed, 5 insertions, 0 deletions

```
diff --git a/net/sctp/outqueue.c b/net/sctp/outqueue.c
index 6fcc4ff97f9453..dc29ac0f8d3f80 100644
--- a/net/sctp/outqueue.c
+++ b/net/sctp/outqueue.c
@@ -403,6 +403,11 @@ static int sctp_prsctp_prune_unsent(struct sctp_association *asoc,
                sout = SCTP_SO(&asoc->stream, chk->sinfo.sinfo_stream);
                sout->ext->abandoned_unsent[SCTP_PR_INDEX(PRIO)]++;

+               /* clear out_curr if all frag chunks are pruned */
+               if (asoc->stream.out_curr == sout &&
+                   list_is_last(&chk->frag_list, &chk->msg->chunks))
+                       asoc->stream.out_curr = NULL;
+
                msg_len -= chk->skb->truesize + sizeof(struct sctp_chunk);
                sctp_chunk_free(chk);
                if (msg_len <= 0)
```