OsmoMGW - Bug #2625

osmo-mgw leaks host data when forwarding RTP packets

11/08/2017 03:31 PM - pespin

Status:	Closed	**Start date:**	11/08/2017
Priority:	Normal	**Due date:**	
Assignee:	dexter	**% Done:**	100%
Category:			
Target version:			

Description

I was testing the new osmo-mgw+osmo-bsc from today's master (54dd4b3f72d90dfbed19ffa7b1e98112add067a6). I can place the call (from msA->msB, the other way it didn't work due to some sccp paging bug according to dexter), but no audio is heard.

Looking at the pcap traces with dexter, everything is fine, all the endpoints and connections are created and handled correctly, and RTP from msA reaches msB and the opposite too. However, no audio can be heard during the call.

It seems the RTP packets going osmo-bts=>osmo-mgw are 87 bytes long, which seems fine, but once they leave the osmo-mgw => osmo-mgcp, then size explodes to 4138 bytes, and the packet contains the initial data + random memory, which in my case contains filesystem paths from my workstation.

So, conclusion, there seems to be some reading out of buffer bounds in the code path in osmo-mgw which receives RTP packets and forwards it. I attach a sample pcap file showing the issue.

Related issues:

Related to OsmoGSMTester - Bug #2626: osmo-gsm-tester: Add osmo-mgw support	**Closed**	**11/08/2017**
Related to OsmoBTS - Bug #2624: osmo-bts aborts: Not enough tailroom msgb_put	**Closed**	**11/08/2017**

History

#1 - 11/08/2017 03:59 PM - pespin

- Related to Bug #2626: osmo-gsm-tester: Add osmo-mgw support added

#2 - 11/08/2017 03:59 PM - pespin

- Related to Bug #2624: osmo-bts aborts: Not enough tailroom msgb_put added

#3 - 11/08/2017 04:01 PM - dexter

- Status changed from New to In Progress

- % Done changed from 0 to 100

The excess data we see in the trace is data from the stack from previous memory usage, its not overflowing anything, but it uses sizeof(buf) as length for the packet that is sent. I have corrected this now.

The patch is up for review: https://gerrit.osmocom.org/4741

#4 - 11/08/2017 04:13 PM - pespin

The patch fixes the issue for me. We can close the issue once it's merged.

#5 - 11/10/2017 11:05 AM - dexter

- Status changed from In Progress to Resolved

#6 - 02/06/2018 08:26 AM - laforge

- Status changed from Resolved to Closed

Files

wrong_size_rtp3.pcapng	106 KB	11/08/2017	pespin