[Live-devel] Live555 Assertion Violation bug

Ba Jinsheng bajinsheng at u.nus.edu
Thu Aug 12 07:19:39 PDT 2021

- Previous message (by thread): [Live-devel] HLSProxy
- Next message (by thread): [Live-devel] Live555 Assertion Violation bug
- **Messages sorted by:** [date] [thread] [subject] [author]

Dear Ross Finlayson,

There may be an assertion violation bug.

When sending multiple SETUP and PLAY commands, the live555 may violate this assertion: liveMedia/FramedSource.cpp:65
Then it outputs "FramedSource[0x610000000440]::getNextFrame(): attempting to read more than once at the same time!" and aborts itself.

The call stack of the exit point:

```
    #6 0x64fafa in UsageEnvironment::internalError() /home/ubuntu/experiments/live555-libfuzzer/UsageEnvironment/UsageEnvironment.cpp:42:3
    #7 0x5502d5 in FramedSource::getNextFrame(unsigned char*, unsigned int, void (*)(void*, unsigned int, unsigned int, timeval, unsigned int), void*, void (*)(void*), void*)
/home/ubuntu/experiments/live555-libfuzzer/liveMedia/FramedSource.cpp:65:13
    #8 0x613e63 in StreamParser::ensureValidBytes1(unsigned int) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/StreamParser.cpp:156:17
    #9 0x558f35 in StreamParser::ensureValidBytes(unsigned int) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/./StreamParser.hh:125:5
    #10 0x558f35 in StreamParser::test4Bytes() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/./StreamParser.hh:54:5
    #11 0x558f35 in MPEGProgramStreamParser::parsePackHeader() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/MPEG1or2Demux.cpp:397:19
    #12 0x557b6e in MPEGProgramStreamParser::parse() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/MPEG1or2Demux.cpp:358:2
    #13 0x557b6e in MPEG1or2Demux::continueReadProcessing() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/MPEG1or2Demux.cpp:236:50
    #14 0x55c946 in MPEG1or2DemuxedElementaryStream::doGetNextFrame() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/MPEG1or2DemuxedElementaryStream.cpp:45:19
    #15 0x613e63 in StreamParser::ensureValidBytes1(unsigned int) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/StreamParser.cpp:156:17
    #16 0x572bb6 in StreamParser::ensureValidBytes(unsigned int) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/./StreamParser.hh:125:5
    #17 0x572bb6 in StreamParser::test4Bytes() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/./StreamParser.hh:54:5
    #18 0x572bb6 in MPEG1or2AudioStreamParser::parse(unsigned int&) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/MPEG1or2AudioStreamFramer.cpp:184:34
    #19 0x571f8f in MPEG1or2AudioStreamFramer::continueReadProcessing() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/MPEG1or2AudioStreamFramer.cpp:134:41
    #20 0x571f8f in MPEG1or2AudioStreamFramer::doGetNextFrame() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/MPEG1or2AudioStreamFramer.cpp:94:3
    #21 0x5d1ac4 in MultiFramedRTPSink::packFrame() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/MultiFramedRTPSink.cpp:223:14
    #22 0x5d11b4 in MultiFramedRTPSink::buildAndSendPacket(unsigned char) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/MultiFramedRTPSink.cpp:199:3
    #23 0x5d11b4 in MultiFramedRTPSink::continuePlaying() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/MultiFramedRTPSink.cpp:159:3
    #24 0x5e8085 in StreamState::startPlaying(Destinations*, unsigned int, void (*)(void*), void*, void (*)(void*, unsigned char), void*) /home/ubuntu/experiments/live555-
libfuzzer/liveMedia/OnDemandServerMediaSubsession.cpp:558:17
    #25 0x5e7796 in OnDemandServerMediaSubsession::startStream(unsigned int, void*, void (*)(void*), void*, unsigned short&, unsigned int&, void (*)(void*, unsigned char), void*)
/home/ubuntu/experiments/live555-libfuzzer/liveMedia/OnDemandServerMediaSubsession.cpp:215:18
    #26 0x4e75c0 in RTSPServer::RTSPClientSession::handleCmd_PLAY(RTSPServer::RTSPClientConnection*, ServerMediaSubsession*, char const*) /home/ubuntu/experiments/live555-
libfuzzer/liveMedia/RTSPServer.cpp:1861:36
    #27 0x4e569e in RTSPServer::RTSPClientSession::handleCmd_withinSession(RTSPServer::RTSPClientConnection*, char const*, char const*, char const*, char const*)
/home/ubuntu/experiments/live555-libfuzzer/liveMedia/RTSPServer.cpp
    #28 0x4dffc6 in RTSPServer::RTSPClientConnection::handleRequestBytes(int) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/RTSPServer.cpp:927:22
    #29 0x4d1e2e in GenericMediaServer::ClientConnection::incomingRequestHandler() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/GenericMediaServer.cpp:291:3
    #30 0x4d1e2e in GenericMediaServer::ClientConnection::incomingRequestHandler(void*, int) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/GenericMediaServer.cpp:284:15
    #31 0x645f85 in BasicTaskScheduler::SingleStep(unsigned int) /home/ubuntu/experiments/live555-libfuzzer/BasicUsageEnvironment/BasicTaskScheduler.cpp:171:2
    #32 0x64e4aa in BasicTaskScheduler0::doEventLoop(char volatile*) /home/ubuntu/experiments/live555-libfuzzer/BasicUsageEnvironment/BasicTaskScheduler0.cpp:80:5
```

To reproduce it, please download the attachment:

  1. Build the docker image:

```
docker build . -t live555_bug
```

  1. Start a container on the image and open two terminals.
  2. In one terminal, run the live555:

```
cd live/testProgs/; ./testOnDemandRTSPServer
```

  1. On the other terminal, run the poc:

```
python3 poc.py
```

Then the testOnDemandRTSPServer aborts.

Best regards,
Jinsheng Ba

```
-------------- next part --------------
An HTML attachment was scrubbed...
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210812/5bf95e61/attachment.htm>
-------------- next part --------------
A non-text attachment was scrubbed...
Name: live555_assertion.zip
Type: application/x-zip-compressed
Size: 1442 bytes
Desc: live555_assertion.zip
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210812/5bf95e61/attachment.bin>
```

- Previous message (by thread): [Live-devel] HLSProxy
- Next message (by thread): [Live-devel] Live555 Assertion Violation bug
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the live-devel mailing list