[Live-devel] Memory Leak in AC3AudioStreamFramer

Ba Jinsheng bajinsheng at u.nus.edu
Thu Aug 12 18:56:47 PDT 2021

- Previous message (by thread): [Live-devel] Live555 Assertion Violation bug
- Next message (by thread): [Live-devel] Memory Leak in AC3AudioStreamFramer
- **Messages sorted by:** [date] [thread] [subject] [author]

Dear Ross Finlayson,

Sorry for many emails and thanks for your reply.

I want to report another memory leak bug in the AC3AudioStreamFramer.

In liveMedia/AC3AudioStreamFramer.cpp:306, fSavedFrame pointer is assigned to a new allocated heap memory. There are two delete[] operations to free this memory:
AC3AudioStreamParser::parseFrame() and AC3AudioStreamParser::onSavedFrameClosurel().
However, sometimes, the class destructor function AC3AudioStreamFramer::~AC3AudioStreamFramer() is executed before the two delete[] operations and incurs the leak of the heap memory fSavedFrame points to.

Mass memory leaks may incur DoS attack and crash the server.

The call stack of the memory leak:

```
Direct leak of 4000 byte(s) in 1 object(s) allocated from:
    #0 0x4c751d in operator new[](unsigned long) (/home/ubuntu/experiments/live555-libfuzzer/testProgs/testOnDemandRTSPServer+0x4c751d)
    #1 0x59b65a in AC3AudioStreamParser::readAndSaveAFrame() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/AC3AudioStreamFramer.cpp:306:17
    #2 0x59b65a in AC3AudioStreamFramer::samplingRate() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/AC3AudioStreamFramer.cpp:112:14
    #3 0x52b316 in AC3AudioFileServerMediaSubsession::createNewRTPSink(Groupsock*, unsigned char, FramedSource*) /home/ubuntu/experiments/live555-
libfuzzer/liveMedia/AC3AudioFileServerMediaSubsession.cpp:60:22
    #4 0x5e5635 in OnDemandServerMediaSubsession::sdpLines(int) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/OnDemandServerMediaSubsession.cpp:71:29
    #5 0x51da33 in ServerMediaSession::generateSDPDescription(int) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/ServerMediaSession.cpp:254:42
    #6 0x4d9682 in RTSPServer::RTSPClientConnection::handleCmd_DESCRIBE_afterLookup(ServerMediaSession*) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/RTSPServer.cpp:380:31
    #7 0x4d82a7 in RTSPServer::RTSPClientConnection::handleCmd_DESCRIBE(char const*, char const*, char const*) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/RTSPServer.cpp:356:14
    #8 0x4df930 in RTSPServer::RTSPClientConnection::handleRequestBytes(int) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/RTSPServer.cpp:796:2
    #9 0x4d1e2e in GenericMediaServer::ClientConnection::incomingRequestHandler() /home/ubuntu/experiments/live555-libfuzzer/liveMedia/GenericMediaServer.cpp:291:3
    #10 0x4d1e2e in GenericMediaServer::ClientConnection::incomingRequestHandler(void*, int) /home/ubuntu/experiments/live555-libfuzzer/liveMedia/GenericMediaServer.cpp:284:15
    #11 0x645f35 in BasicTaskScheduler::SingleStep(unsigned int) /home/ubuntu/experiments/live555-libfuzzer/BasicUsageEnvironment/BasicTaskScheduler.cpp:171:2
    #12 0x64e45a 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
```

Now we can see the memory usage from the top command:
[cid:image001.png at 01D79028.E331EAF0]

1. On the other terminal, run the poc:

```
./poc.sh
```

After 20 seconds, the memory usage:
[cid:image002.png at 01D79029.870D3E90]

Best regards,
Jinsheng Ba

```
-------------- next part --------------
An HTML attachment was scrubbed...
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210813/c58386c8/attachment-0001.htm>
-------------- next part --------------
A non-text attachment was scrubbed...
Name: image001.png
Type: image/png
Size: 4294 bytes
Desc: image001.png
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210813/c58386c8/attachment-0002.png>
-------------- next part --------------
A non-text attachment was scrubbed...
Name: image002.png
Type: image/png
Size: 4314 bytes
Desc: image002.png
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210813/c58386c8/attachment-0003.png>
-------------- next part --------------
A non-text attachment was scrubbed...
Name: live555_leak.zip
Type: application/x-zip-compressed
Size: 1442 bytes
Desc: live555_leak.zip
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210813/c58386c8/attachment-0001.bin>
```

- Previous message (by thread): [Live-devel] Live555 Assertion Violation bug
- Next message (by thread): [Live-devel] Memory Leak in AC3AudioStreamFramer
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the live-devel mailing list