[Live-devel] Stack Overflow in FD_SET()

Ba Jinsheng bajinsheng at u.nus.edu
Tue Aug 3 07:52:09 PDT 2021

- Previous message (by thread): [Live-devel] RTSP Metadata
- Next message (by thread): [Live-devel] Stack Overflow in FD_SET()
- **Messages sorted by:** [date] [thread] [subject] [author]

To whom it may concern,

I am a researcher working on fuzzing and I would like to report a stack overflow bug in live555.

When a large number of requests for the same MP3 file in a short time, the live555 quickly open the same MP3 file multiple time. Then, the value of the newly assigned file descriptor for the mp3 file quickly exceed 1024 here: liveMedia/MP3FileSource.cpp: 46
It uses "select()" system call to check if the file is readable. However, the "select()" usually support maximum 1024 file descriptor value, so it incurs a stack overflow in FD_SET: MP3StreamState.cpp: 343

This is the output from AddressSanitizer:
[cid:image001.jpg at 01D788BA.302143E0]

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:

```
./poc.sh
```

Then the testOnDemandRTSPServer would crash in several seconds.

Best regards
Jinsheng Ba

An HTML attachment was scrubbed...
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210803/7ede9297/attachment-0001.htm>

A non-text attachment was scrubbed...
Name: image001.jpg
Type: image/jpeg
Size: 136257 bytes
Desc: image001.jpg
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210803/7ede9297/attachment-0001.jpg>

A non-text attachment was scrubbed...
Name: overflow_poc_live555.zip
Type: application/x-zip-compressed
Size: 1555 bytes
Desc: overflow_poc_live555.zip
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210803/7ede9297/attachment-0001.bin>

- Previous message (by thread): [Live-devel] RTSP Metadata
- Next message (by thread): [Live-devel] Stack Overflow in FD_SET()
- **Messages sorted by:** [date] [thread] [subject] [author]
