[Live-devel] UAF in Live555

Ba Jinsheng bajinsheng at u.nus.edu
Fri Aug 6 07:58:20 PDT 2021

- Previous message (by thread): [Live-devel] Stack Overflow in FD_SET()
- Next message (by thread): [Live-devel] UAF in Live555
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Hi,

I want to report another Use-after-free bug in live555:

The bug happens when setting up the same stream twice:
After sending a "DESCRIBE" command, we send a "SETUP" command, then use the returned "Session ID" to send another "SETUP" command to trigger this UAF:
[cid:image001.png at 01D78B15.663BFB20]


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 crashes.


Best regards,
Jinsheng Ba

-------------- next part --------------
An HTML attachment was scrubbed...
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210806/6ca19dc3/attachment-0001.htm>
-------------- next part --------------
A non-text attachment was scrubbed...
Name: image001.png
Type: image/png
Size: 89162 bytes
Desc: image001.png
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210806/6ca19dc3/attachment-0001.png>
-------------- next part --------------
A non-text attachment was scrubbed...
Name: UAF_POC.zip
Type: application/x-zip-compressed
Size: 333343 bytes
Desc: UAF_POC.zip
URL: <http://lists.live555.com/pipermail/live-devel/attachments/20210806/6ca19dc3/attachment-0001.bin>
```

- Previous message (by thread): [Live-devel] Stack Overflow in FD_SET()
- Next message (by thread): [Live-devel] UAF in Live555
- **Messages sorted by:** [date] [thread] [subject] [author]
