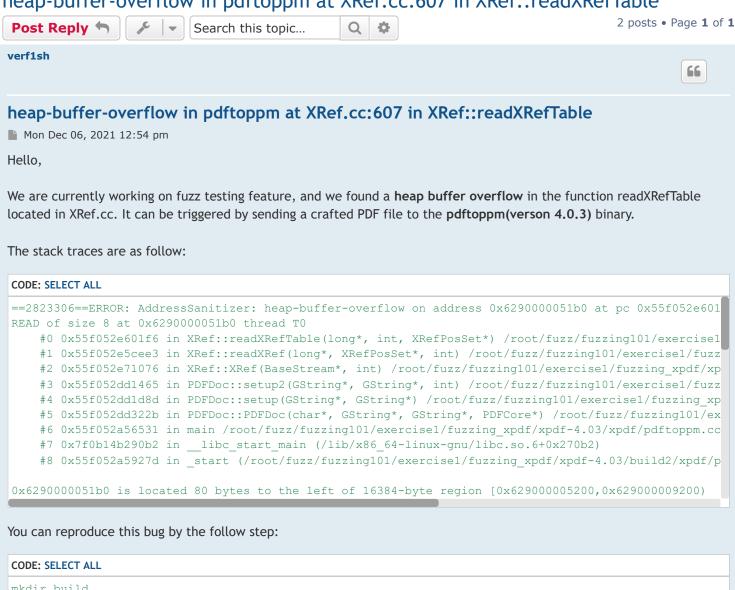


heap-buffer-overflow in pdftoppm at XRef.cc:607 in XRef::readXRefTable



```
mkdir build
cd build
export CC=afl-clang-fast
export CXX=afl-clang-fast++
cmake ..

AFL_USE_ASAN=1 make -j8
./pdftoppm ./poc_ppm 3.ppm
```

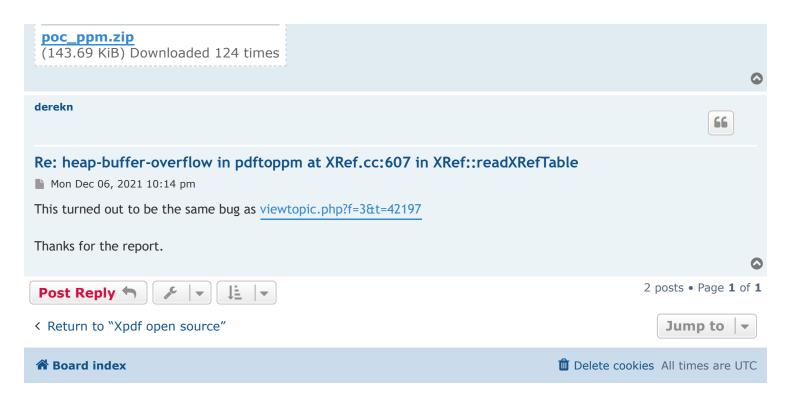
You can download this PoC file at ATTACHMENTS

Environment

- Tested on Ubuntu 20.04.3 LTS x86_64, AFL++
- gcc version 10.3.0
- xpdf version: [xpdf 4.3.0](https://dl.xpdfreader.com/xpdf-4.03.tar.gz)

Thank you.

ATTACHMENTS



Powered by phpBB® Forum Software © phpBB Limited Privacy | Terms