New issue

Jump to bottom

Stack-buffer-overflow-XRef-fetch #45

Open Aurorainfinity opened this issue on Jul 9, 2020 · 0 comments

Aurorainfinity commented on Jul 9, 2020

```
$ ./pdf2json 01-Stack-buffer-overflow-XRef-fetch.pdf
ASAN:SIGSEGV
=================================================================
==89368==ERROR: AddressSanitizer: stack-overflow on address 0x7ffc9d6bcfe0 (pc 0x7f2cf5cba26e bp 0x000000000018 sp 0x7ffc9d6bcfd0 T0)
    #0 0x7f2cf5cba26d  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xb026d)
    #1 0x7f2cf5cb9d67  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xafd67)
    #2 0x7f2cf5c2cf4f  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x22f4f)
    #3 0x7f2cf5ca34fe in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x994fe)
    #4 0x4345c4 in XRef::fetch(int, int, Object*) /home/test/pdf2json_tmp/xpdf/XRef.cc:839
    #5 0x434835 in ObjectStream::ObjectStream(XRef*, int) /home/test/pdf2json_tmp/xpdf/XRef.cc:84
    #6 0x4345d6 in XRef::fetch(int, int, Object*) /home/test/pdf2json_tmp/xpdf/XRef.cc:839
    #7 0x434835 in ObjectStream::ObjectStream(XRef*, int) /home/test/pdf2json_tmp/xpdf/XRef.cc:84
    #8 0x4345d6 in XRef::fetch(int, int, Object*) /home/test/pdf2json_tmp/xpdf/XRef.cc:839
    #9 0x434835 in ObjectStream::ObjectStream(XRef*, int) /home/test/pdf2json_tmp/xpdf/XRef.cc:84
    #10 0x4345d6 in XRef::fetch(int, int, Object*) /home/test/pdf2json_tmp/xpdf/XRef.cc:839
    #11 0x434835 in ObjectStream::ObjectStream(XRef*, int) /home/test/pdf2json_tmp/xpdf/XRef.cc:84
```

ref:https://github.com/Aurorainfinity/Poc/tree/master/pdf2json
01-Stack-buffer-overflow-XRef-fetch.pdf

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant