Aurorainfinity add pdf2json poc readme ... on Jul 9, 2020 History

..

00-NULL-pointer-dereference-ObjectStream-getObject.pdf	2 years ago
01-Stack-buffer-overflow-XRef-fetch.pdf	2 years ago
readme.md	2 years ago

readme.md

00-NULL-pointer-dereference-ObjectStream-getObject

```
$ pdf2json 00-NULL-pointer-dereference-ObjectStream-getObject.pdf

Error (1853): Dictionary key must be a name object
Error (1860): Dictionary key must be a name object
ASAN:SIGSEGV
=================================================================
==88712==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x000000432f60 bp 0x7ffe1f9cf650 sp 0x7ffe1f9cf5b8 T0)
    #0 0x432f5f in ObjectStream::getObject(int, int, Object*) /home/test/pdf2json_tmp/xpdf/XRef.cc:183
    #1 0x4345ec in XRef::fetch(int, int, Object*) /home/test/pdf2json_tmp/xpdf/XRef.cc:841
    #2 0x411283 in Object::dictLookup(char*, Object*) /home/test/pdf2json_tmp/xpdf/Object.h:253
    #3 0x411283 in Catalog::Catalog(XRef*) /home/test/pdf2json_tmp/xpdf/Catalog.cc:51
    #4 0x427fe0 in PDFDoc::setup(GString*, GString*) /home/test/pdf2json_tmp/xpdf/PDFDoc.cc:201
    #5 0x42815b in PDFDoc::PDFDoc(GString*, GString*, GString*, void*) /home/test/pdf2json_tmp/xpdf/PDFDoc.cc:101
    #6 0x402856 in main /home/test/pdf2json_tmp/src/pdf2json.cc:159
    #7 0x7fd2eaec383f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #8 0x403788 in _start (/home/test/pdf2json_tmp/src/pdf2json+0x403788)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/test/pdf2json_tmp/xpdf/XRef.cc:183 ObjectStream::getObject(int, int, Object*)
==88712==ABORTING
```

01-Stack-buffer-overflow-XRef-fetch

```
$ 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
```