New issue

Jump to bottom

NULL-pointer-dereference-ObjectStream-getObject #44

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

Aurorainfinity commented on Jul 9, 2020

```
$  ./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
```

ref:https://github.com/Aurorainfinity/Poc/tree/master/pdf2json
00-NULL-pointer-dereference-ObjectStream-getObject.pdf

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant