New issue

Jump to bottom

SEGV on ObjectStream::getObject #26

Open **strongcourage** opened this issue on May 27, 2019 · 0 comments

strongcourage commented on May 27, 2019 • edited

Hi,

Our fuzzer found a crash due to an invalid read on the function ObjectStream::getObject (the latest commit `b671b64` on master - version 0.70).

PoC: https://github.com/strongcourage/PoCs/blob/master/pdf2json_b671b64/PoC_segv_ObjectStream::getObject

Valgrind says

```
valgrind pdf2json $PoC /dev/null
==440== Memcheck, a memory error detector
==440== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
==440== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
==440== Command: ./pdf2json ./PoC_segv_ObjectStream::getObject /dev/null
==440==
==440== Invalid read of size 4
==440==    at 0x43D665: ObjectStream::getObject(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x43FB45: XRef::fetch(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x4094D9: XRef::getCatalog(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x407B94: Catalog::Catalog(XRef*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x42B5FA: PDFDoc::setup(GString*, GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x42B3B4: PDFDoc::PDFDoc(GString*, GString*, GString*, void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x402163: main (pdf2json.cc:159)
==440==  Address 0x10 is not stack'd, malloc'd or (recently) free'd
==440==
==440==
==440== Process terminating with default action of signal 11 (SIGSEGV)
==440==  Access not within mapped region at address 0x10
==440==    at 0x43D665: ObjectStream::getObject(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x43FB45: XRef::fetch(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x4094D9: XRef::getCatalog(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x407B94: Catalog::Catalog(XRef*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x42B5FA: PDFDoc::setup(GString*, GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x42B3B4: PDFDoc::PDFDoc(GString*, GString*, GString*, void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==440==    by 0x402163: main (pdf2json.cc:159)
==440==  If you believe this happened as a result of a stack
==440==  overflow in your program's main thread (unlikely but
==440==  possible), you can try to increase the size of the
==440==  main thread stack using the --main-stacksize= flag.
==440==  The main thread stack size used in this run was 8388608.
==440==
==440== HEAP SUMMARY:
==440==     in use at exit: 204,239 bytes in 1,701 blocks
==440==   total heap usage: 1,792 allocs, 91 frees, 353,981 bytes allocated
==440==
==440== LEAK SUMMARY:
==440==    definitely lost: 0 bytes in 0 blocks
==440==    indirectly lost: 0 bytes in 0 blocks
==440==      possibly lost: 0 bytes in 0 blocks
==440==    still reachable: 204,239 bytes in 1,701 blocks
==440==         suppressed: 0 bytes in 0 blocks
==440== Rerun with --leak-check=full to see details of leaked memory
==440==
==440== For counts of detected and suppressed errors, rerun with: -v
==440== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
Segmentation fault
```

Thanks,
Manh Dung

strongcourage changed the title ~~Segmentation fault on ObjectStream::getObject~~ **SEGV on ObjectStream::getObject** on May 29, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant