SEGV (NULL pointer dereference) on EmbedStream::getChar #29

⊙ Open **strongcourage** opened this issue on May 28, 2019 · 0 comments

strongcourage commented on May 28, 2019

Hi,

Our fuzzer found a crash due to a NULL pointer dereference bug on the function EmbedStream::getChar (the latest commit `b671b64` on master - version 0.70).

PoC: https://github.com/strongcourage/PoCs/blob/master/pdf2json_b671b64/PoC_npd_EmbedStream::getChar

Valgrind says:

```
valgrind pdf2json $PoC /dev/null
==23888== Memcheck, a memory error detector
==23888== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
==23888== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
==23888== Command: ./pdf2json ./PoC_npd_EmbedStream::getChar /dev/null
==23888==
Error: May not be a PDF file (continuing anyway)
Error: PDF file is damaged - attempting to reconstruct xref table...
Error (15671): Dictionary key must be a name object
Error (15674): Dictionary key must be a name object
Error (1930): Dictionary key must be a name object
Error (1933): Dictionary key must be a name object
Error (1935): Dictionary key must be a name object
Error (1937): Dictionary key must be a name object
Error (1940): Dictionary key must be a name object
Error (3436): Illegal character ')'
Error: Unterminated string
Error: Bad image parameters
==23888== Invalid read of size 8
==23888==    at 0x42ECFA: EmbedStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x466405: Gfx::opBeginImage(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x40269A: main (pdf2json.cc:275)
==23888==  Address 0x0 is not stack'd, malloc'd or (recently) free'd
==23888==
==23888==
==23888== Process terminating with default action of signal 11 (SIGSEGV)
==23888==  Access not within mapped region at address 0x0
==23888==    at 0x42ECFA: EmbedStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x466405: Gfx::opBeginImage(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==23888==    by 0x40269A: main (pdf2json.cc:275)
==23888==  If you believe this happened as a result of a stack
==23888==  overflow in your program's main thread (unlikely but
==23888==  possible), you can try to increase the size of the
==23888==  main thread stack using the --main-stacksize= flag.
==23888==  The main thread stack size used in this run was 8388608.
==23888==
==23888== HEAP SUMMARY:
==23888==     in use at exit: 212,135 bytes in 1,754 blocks
==23888==   total heap usage: 1,929 allocs, 175 frees, 301,634 bytes allocated
==23888==
==23888== LEAK SUMMARY:
==23888==    definitely lost: 16 bytes in 1 blocks
==23888==    indirectly lost: 8 bytes in 1 blocks
==23888==      possibly lost: 0 bytes in 0 blocks
==23888==    still reachable: 212,111 bytes in 1,752 blocks
==23888==         suppressed: 0 bytes in 0 blocks
==23888== Rerun with --leak-check=full to see details of leaked memory
==23888==
==23888== For counts of detected and suppressed errors, rerun with: -v
==23888== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
Segmentation fault
```

Thanks,
Manh Dung

strongcourage changed the title ~~Segmentation fault (NULL pointer dereference) on EmbedStream::getChar~~ SEGV (NULL pointer dereference) on EmbedStream::getChar 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