This repository has been archived by the owner before Nov 9, 2022. It is now read-only.

Heap-buffer-overflow-TextPage-dump #11

Open **Aurorainfinity** opened this issue on Jul 5, 2020 · 0 comments

Aurorainfinity commented on Jul 5, 2020

$ ./pdf2xml 01-Heap-buffer-overflow-TextPage-dump.pdf test.xml

```
==36659==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200004405a at pc 0x7fb7e473d9f5 bp 0x7ffc8a9d8c60 sp 0x7ffc8a9d83f0
WRITE of size 11 at 0x60200004405a thread T0
    #0 0x7fb7e473d9f4 in __interceptor_vsprintf (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x619f4)
    #1 0x7fb7e473dcc9 in __interceptor_sprintf (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x61cc9)
    #2 0x419e84 in TextPage::dump(int, int) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:2001
    #3 0x428ec5 in XmlOutputDev::endPage() /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:4155
    #4 0x48e309 in Gfx::~Gfx() /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:591
    #5 0x45633a in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:394
    #6 0x45653e in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*), void*) /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:310
    #7 0x45740d in PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int (*)(void*), void*) /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/PDFDoc.cc:398
    #8 0x407de8 in PDFDocXrce::displayPages(OutputDev*, _xmlNode*, int, int, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/src/PDFDocXrce.cc:34
    #9 0x40943b in main /home/test/pdf2xml_analysis/pdf2xml/src/pdftoxml.cc:409
    #10 0x7fb7e321182f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #11 0x403d28 in _start (/home/test/pdf2xml_analysis/pdf2xml/pdf2xml+0x403d28)

0x60200004405a is located 0 bytes to the right of 10-byte region [0x602000044050,0x60200004405a)
allocated by thread T0 here:
    #0 0x7fb7e4774602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x416b22 in TextPage::dump(int, int) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1652
    #2 0x428ec5 in XmlOutputDev::endPage() /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:4155
    #3 0x48e309 in Gfx::~Gfx() /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:591
    #4 0x45653e in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*), void*) /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:310

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 __interceptor_vsprintf
Shadow bytes around the buggy address:
  0x0c04800007b0: fa fa 00 fa fa fa 00 02 fa fa 00 fa fa fa 00 00
  0x0c04800007c0: fa fa 00 fa fa fa fd fa fa fa 00 fa fa fa 00 00
  0x0c04800007d0: fa fa fd fa fa fa fd fd fa fa 06 fa fa fa 03 fa
  0x0c04800007e0: fa fa fd fd fa fa fd fa fa fa fd fd fa fa 06 fa
  0x0c04800007f0: fa fa 04 fa fa fa fd fd fa fa fd fa fa fa fd fd
=>0x0c0480000800: fa fa 06 fa fa fa 05 fa fa fa 00[02]fa fa 00 fa
  0x0c0480000810: fa fa fd fa fa fa 00 fa fa fa fd fa fa fa fd fa
  0x0c0480000820: fa fa fd fa fa fa fd fa fa fa fd fa fa fa 05 fa
  0x0c0480000830: fa fa 07 fa fa fa 00 fa fa fa 02 fa fa fa 00 fa
  0x0c0480000840: fa fa 02 fa fa fa 02 fa fa fa 00 fa fa fa 02 fa
  0x0c0480000850: fa fa 00 fa fa fa 02 fa fa fa 02 fa fa fa 00 fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
==36659==ABORTING
```

01-Heap-buffer-overflow-TextPage-dump.pdf

ref:https://github.com/Aurorainfinity/Poc/tree/master/pdf2xml

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant