flexpaper / pdf2json Public

Code Issues 35 Pull requests Actions Projects Wiki ···

New issue

Jump to bottom

Aborted on DCTStream::decodeImage #32

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

strongcourage commented on May 28, 2019

Hi,

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

PoC: https://github.com/strongcourage/PoCs/blob/master/pdf2json_b671b64/PoC_aborted_DCTStream::decodeImage

Valgrind says:

```
valgrind pdf2json $PoC /dev/null
==17382== Memcheck, a memory error detector
==17382== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
==17382== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
==17382== Command: ./pdf2json ./PoC_aborted_DCTStream::decodeImage /dev/null
==17382==
Error: PDF file is damaged - attempting to reconstruct xref table...
Error (15396): Illegal character <5c> in hex string
Error (15407): Illegal character <78> in hex string
Error (154): Dictionary key must be a name object
Error (165): Dictionary key must be a name object
Error (528): Dictionary key must be a name object
Error (530): Dictionary key must be a name object
Error (532): Dictionary key must be a name object
Error (536): Dictionary key must be a name object
Error (539): Dictionary key must be a name object
Error (545): Dictionary key must be a name object
Error (8015): Command token too long
Error (8139): Missing 'endstream'
Error (1970): Unknown DCT marker <75>
==17382== Invalid read of size 4
==17382==    at 0x435431: DCTStream::decodeImage() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432C6C: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==  Address 0x5b5bf10 is 0 bytes after a block of size 100,352 alloc'd
==17382==    at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==17382==    by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432BC5: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==
==17382== Invalid read of size 4
==17382==    at 0x435452: DCTStream::decodeImage() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432C6C: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==  Address 0x5b5bf14 is 4 bytes after a block of size 100,352 alloc'd
==17382==    at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==17382==    by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432BC5: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==
==17382== Invalid read of size 4
==17382==    at 0x43546F: DCTStream::decodeImage() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432C6C: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==  Address 0x5b5bf18 is 8 bytes after a block of size 100,352 alloc'd
==17382==    at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==17382==    by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432BC5: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==
==17382== Invalid read of size 4
==17382==    at 0x43548C: DCTStream::decodeImage() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432C6C: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==  Address 0x5b5bf1c is 12 bytes after a block of size 100,352 alloc'd
==17382==    at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==17382==    by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432BC5: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==
==17382== Invalid read of size 4
==17382==    at 0x4354A9: DCTStream::decodeImage() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432C6C: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==  Address 0x5b5bf20 is 16 bytes after a block of size 100,352 alloc'd
==17382==    at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==17382==    by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432BC5: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==
==17382== Invalid read of size 4
==17382==    at 0x4354C6: DCTStream::decodeImage() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432C6C: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==  Address 0x5b5bf24 is 20 bytes after a block of size 100,352 alloc'd
==17382==    at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==17382==    by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432BC5: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==
==17382== Invalid read of size 4
==17382==    at 0x4354E3: DCTStream::decodeImage() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432C6C: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==  Address 0x5b5bf28 is 24 bytes after a block of size 100,352 in arena "client"
==17382==
==17382== Invalid read of size 4
==17382==    at 0x435500: DCTStream::decodeImage() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432C6C: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==  Address 0x5b5bf2c is 28 bytes after a block of size 100,352 in arena "client"
==17382==
==17382== Invalid read of size 1
==17382==    at 0x43698B: DCTStream::transformDataUnit(unsigned short*, int*, unsigned char*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x43555E: DCTStream::decodeImage() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432C6C: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==  Address 0x6feabb is not stack'd, malloc'd or (recently) free'd
==17382==
==17382==
==17382== Process terminating with default action of signal 11 (SIGSEGV)
==17382==  Access not within mapped region at address 0x6FEABB
==17382==    at 0x43698B: DCTStream::transformDataUnit(unsigned short*, int*, unsigned char*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x43555E: DCTStream::decodeImage() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x432C6C: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    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)
==17382==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==17382==    by 0x40269A: main (pdf2json.cc:275)
==17382==  If you believe this happened as a result of a stack
==17382==  overflow in your program's main thread (unlikely but
==17382==  possible), you can try to increase the size of the
==17382==  main thread stack using the --main-stacksize= flag.
==17382==  The main thread stack size used in this run was 8388608.
==17382==
==17382== HEAP SUMMARY:
==17382==     in use at exit: 518,164 bytes in 1,769 blocks
==17382==   total heap usage: 1,978 allocs, 209 frees, 609,684 bytes allocated
==17382==
==17382== LEAK SUMMARY:
==17382==    definitely lost: 16 bytes in 1 blocks
==17382==    indirectly lost: 8 bytes in 1 blocks
==17382==      possibly lost: 0 bytes in 0 blocks
==17382==    still reachable: 518,140 bytes in 1,767 blocks
==17382==         suppressed: 0 bytes in 0 blocks
==17382== Rerun with --leak-check=full to see details of leaked memory
==17382==
==17382== For counts of detected and suppressed errors, rerun with: -v
==17382== ERROR SUMMARY: 57 errors from 9 contexts (suppressed: 0 from 0)
Segmentation fault
```

Thanks,
Manh Dung

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant