Jump to bottom New issue

SEGV on CCITTFaxStream::lookChar #36

Open strongcourage opened this issue on May 29, 2019 · 0 comments

```
strongcourage commented on May 29, 2019
Hi.
Our fuzzer found a crash due to an invalid write on the function CCITTFaxStream::lookChar (the latest commit b671b64 on master - version 0.70)
PoC: https://github.com/strongcourage/PoCs/blob/master/pdf2json b671b64/PoC seg CCITTFaxStream::lookChar
Valorind says:
   valgrind pdf2json $PoC /dev/null
==15436== Memcheck, a memory error detector
   ==15436== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
    ==15436== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
   ==15436== Command: ./pdf2json ./PoC segv CCITTFaxStream::lookChar /dev/null
   ==15436== Invalid write of size 2
                     at 0x431600: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
   ==15436==
   ==15436==
                     by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4884FD: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
   ==15436==
                     by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489825: Parser::get0bj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
   ==15436==
   ==15436==
                     by 0x454311: Gfx::display(Object*, Int) (in /home/dungnguyen/PoCs/pdf2json) by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
   ==15436==
==15436==
   /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                     by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
    ==15436==
   at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                     by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
   ==15436==
                     by 0x43051F: CCITTFaxStream::CCITTFaxStream(Stream*, int, int, int, int, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
                     ==15436==
==15436==
   ==15436==
==15436==
   ==15436== by 0x43FA44: XMef::fetch(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436= by 0x42B44: XMef::fetch(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436= by 0x42B49: Object::fetch(XMef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42B49: Object::fetch(XMef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
    ==15436==
                     by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
   /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
   ==15436== Invalid read of size 2
   ==15436==
                   at 0x43162B: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                     by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json
by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
    ==15436==
                     by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
by 0x4896F: Lexer::getObj(Object*) (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
by 0x4884FD: Lexer::getObj(Object*) (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
by 0x4895C19: Parser::shift() (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
by 0x4895C29: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int) (in /home/dungnguyen/PoCS/pdf2json_b671b64/pdf2json)
by 0x458759: Gfx::go(int) (in /home/dungnguyen/PoCS/pdf2json_b671b64/pdf2json)
   ==15436==
   ==15436==
   ==15436==
   ==15436==
==15436==
   ==15436==
                      by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436== Address 0x5b100bc is 0 bytes after a block of size 108 alloc'd
==15436== at 0x4C2D88F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                     by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x43051F: CCITTFaxStream::CCITTFaxStream(Stream*, int, int, int, int, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
   ==15436==
   ==15436==
                     by 0x42CE76: Stream::makeFilter(char*, Stream*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                     by 0x42CEAR: Stream::makerFilet(char', object') (in /nome/dunginguyen/rocs/pdf2json_b671b64/pdf2json)
by 0x42CEAR: Stream::makeStream(Object*) (in /nome/dunginguyen/rocs/pdf2json_b671b64/pdf2json)
by 0x489AFF: Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dunginguyen/Pocs/pdf2json_b671b64/pdf2json)
by 0x489AF8: Parser::getObj(Object*) (unsigned char*, CryptAlgorithm, int, int, int) (in /home/dunginguyen/Pocs/pdf2json_b671b64/pdf2json)
by 0x48AF44: XRef::fetch(int, int, Object*) (in /home/dunginguyen/Pocs/pdf2json_b671b64/pdf2json)
by 0x428AA9: Object::fetch(XRef*, Object*) (in /home/dunginguyen/Pocs/pdf2json_b671b64/pdf2json)
   ==15436==
   ==15436==
   ==15436==
   ==15436==
   by 0x42A14A: Page::display(OutputDev*, double, double, int. int. Links*, int. Catalog*, int (*)(void*), void*) (in
   ==15436==
   /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
    ==15436==
   ==15436== Invalid read of size 2
==15436== at 0x43154B: CCITTF
                     at 0x43154B: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                     by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
    ==15436==
                     by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4884FD: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
                     by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489825: Parser::get0bj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==15436==
    ==15436==
                     by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42439E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
   ==15436==
    ==15436==
   ==15436==
   /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
   /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
    ==15436== Address 0x5b100bc is 0 bytes after a block of size 108 alloc'd
```

```
==15436==
                      at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==15436==
                      by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==15436==
                      by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x43E567: CCITTFaxStream::CCITTFaxStream(Stream*, int, int, int, int, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                      by 0x42CE76: Stream::makeFilter(char*, Stream*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x42C6AF: Stream::addFilters(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                      by 0x489AFF: Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x489549: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                      by 0x43FA44: XRef::fetch(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4284A9: Object::fetch(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x428A565: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
==15436==
==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==15436==
==15436== Invalid write of size 2
 ==15436==
                      at 0x431556: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                      by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                      by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==15436==
==15436==
==15436==
                      by 0x4884FD: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x483825: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                      by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyer/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
 ==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
//nome/pumgnguyen/Pocs/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjsom_por/1000/purzjso
                      by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x43051F: CCITTFaxStream::CCITTFaxStream(Stream*, int, int, int, int, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                     by 0x42CF6: Stream::makeFitzer(char*, Stream*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42CF6: Stream::makeFitzer(char*, Stream*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42C6AF: Stream::addFilters(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489AFF: Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489AFF: Parser::gevbloj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x48FA44: XRef::fetch(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
 ==15436==
==15436==
 ==15436==
==15436==
==15436==
                      by 0x4284A9: Object::fetch(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==15436==
                      by 0x42A565: 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)
==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== Invalid read of size 2
==15436==
                      at 0x431581: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                      by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                      by 0x4884FD: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                      by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==15436==
                      by 0x489825: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                      by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
/home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== Address 0x5b100be is 2 bytes after a block of size 100 alloc'd
                     at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                     by 0x48E657: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b071b64/pdf2json)
by 0x48E657: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b071b64/pdf2json)
by 0x48E675: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42E675: Stream::makefilter(farm*, Stream*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42E6AF: Stream::addfilters(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
 ==15436==
==15436==
                      by 0x489AFF: Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x489549: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==15436==
                      by 0x43FA44: XRef::fetch(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42R4A9: Object::fetch(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A565: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
==15436==
==15436==
/home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436== Invalid read of size 2
                      at 0x4315F5: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                      by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x4884FD: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                      by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x489825: Parser::get0bj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                      by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x42ECBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==15436==
==15436== Address 0x5b100be is 2 bytes after a block of size 108 alloc'd
==15436==
                      at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==15436==
                      by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x43e51F: CCITTFaxStream::CCITTFaxStream(Stream*, int, int, int, int, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                      by 0x42CE76: Stream::makeFilter(char*, Stream*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x42C6AF: Stream::addFilters(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x489AFF: Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x489549: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x43FA44: XRef::fetch(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
==15436==
                      by 0x4284A9: Object::fetch(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A565: 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) ==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
Error (5428): Bad white code (000b) in CCITTFax stream
 ==15436== Invalid read of size 2
==15436== at 0x43165C: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                      by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
==15436==
                  by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                  by 0x4884FD: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489825: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                  by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                  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)
                  by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                  by 0x467BC1: Gfx::saveState() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A586: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) (in
==15436==
/home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                  by 0x42ECBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x42EDB4: PDFDoc::displayPages(OutputDev*, int, int, ouble, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                  by 0x40269A: main (pdf2json.cc:275)
==15436==
==15436== Invalid read of size 2
                  at 0x431688: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==15436==
                  by 0x43ADDC: CCITIFaxStream::getChar() (in /home/dungnguyen/POCS/pdf2json_b671b64/pdf2json)
by 0x48P47A: 0bject::streamGetChar() (in /home/dungnguyen/POCS/pdf2json_b671b64/pdf2json)
by 0x48P47A: 0bject::streamGetChar() (in /home/dungnguyen/POCS/pdf2json_b671b64/pdf2json)
by 0x48P47B: Lexer::getChar() (in /home/dungnguyen/POCS/pdf2json_b671b64/pdf2json)
by 0x48P47B: Lexer::getCbj(0bject*) (in /home/dungnguyen/POCS/pdf2json_b671b64/pdf2json)
by 0x48P4C19: Parser::shift() (in /home/dungnguyen/POCS/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
==15436==
==15436==
                  by 0x483825: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
 ==15436==
==15436==
                  by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyer/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
 ==15436==
/home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==15436= by @x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                  by @x42BCBD: PDFDc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436== Address 0x5b1040a is 22 bytes before a block of size 8 alloc'd
                  by 0x40A204: GfxDeviceGrayColorSpace::copy() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                  by 0x41AF23: GfxState::GfxState(GfxState*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x41CDB8: GfxState::copy() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
 ==15436==
                  by 0x41C749: GfxState::save() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x467BC1: Gfx::saveState() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x462B61: Gfx::saveState() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A586: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
==15436==
==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==15436==
                 by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                  by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                  by 0x40269A: main (pdf2json.cc:275)
==15436==
Error (5585): CCITTFax row is wrong length (101)
==15436== Invalid read of size 2
==15436== at 0x4316CF: CCITTFa
                  at 0x4316CF: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                  by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                  by 0x4884FD: Lexer::get0bj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                  by 0x489825: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                  by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                  by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) (in
==15436==
 ==15436==
/home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== bv 0x42BCBD: PDFDoc::displayPage(Out
==15436== by 0x428CBD; PPFD0c::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) ==15436== Address 0x5b1040a is 22 bytes before a block of size 8 alloc'd
                  at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x40A204: GfxDeviceGrayColorSpace::copy() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                  by 0x41AF23: GfxState::GfxState(GfxState*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                  by 0x41CDB8: GfxState::copy() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                  by 0x41C749: GfxState::save() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x467BC1: Gfx::saveState() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x462A586: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
 ==15436==
==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                  by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                  by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, int, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                  by 0x428D48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40269A: main (pdf2json.cc:275)
==15436==
 ==15436== Invalid write of size 2
==15436==
                  at 0x431722: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                  by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==15436==
==15436==
                  by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                  by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                  by 0x4884FD: Lexen::gettoli(Object*) (in /nome/dungngyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4884FD: Lexen::gettobi(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489SES: Parser::get0bi(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454759: 6fx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
==15436==
==15436==
by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                  by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== Address 0x5b1040a is 22 bytes before a block of size 8 alloc'd ==15436== at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==15436==
                  by 0x40A204: GfxDeviceGrayColorSpace::copy() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x41AF23: GfxState::GfxState(GfxState*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                  by 0x41CDB8: GfxState::copy() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x41C749: GfxState::save() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
 ==15436==
==15436==
                  by 0x467BC1: Gfx::saveState() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A586: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== bv 0x42A14A: Page::display(OutputDev
                  by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
==15436==
                 by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                 by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==15436==
                 by 0x40269A: main (pdf2json.cc:275)
==15436==
==15436== Invalid read of size 2
                 at 0x431C78: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                 by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                 by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                 by 0x4884FD: Lexen::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 by 0x489825: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                 by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
/home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
                 by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 by 0x42ECBD: PPFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== Address 0x5b100bc is 0 bytes after a block of size 108 alloc'd
==15436==
==15436==
                 at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 ==15436==
                 by 0x42CE76: Stream::makeFilter(char*, Stream*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42C6AF: Stream::addFilters(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489AFF: Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                 by 0x489549: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                 by 0x43FA44: XRef::fetch(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42R4A9: Object::fetch(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42R4565: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
==15436==
==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== Invalid read of size 2
                valiu read ut 512e 2 at texasticat. CCITIFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x43ADDC: CCITIFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
==15436==
==15436==
                 by 0x4884FD: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==15436==
==15436==
                 by 0x489825: Parser::get0bj(Object*, unsigned char*, CryptAlgorithm, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                 by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyer/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) (in
==15436==
 ==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) ==15436== Address 0x5b100bc is 0 bytes after a block of size 108 alloc'd
==15436==
                 at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                by 0x486567: gmallot (in /nome/dungnguyen/PocSyptr2json_po/los/port_json)
by 0x486567: gmallot (in /home/dungnguyen/PocSyptr2json_po/los/port_json)
by 0x48657: gmallot (in /home/dungnguyen/PocSyptr2json_bof7lb64/pdf2json)
by 0x42657: Stream::akefilter(sar*, Stream*, Object*) (in /home/dungnguyen/PocSyptr2json_bof7lb64/pdf2json)
by 0x426647: Stream::addfilters(Object*) (in /home/dungnguyen/PocSyptr2json_bof7lb64/pdf2json)
by 0x426647: Stream::addfilters(Object*) (in /home/dungnguyen/PocSyptr2json_bof7lb64/pdf2json)
==15436==
==15436==
==15436==
==15436==
==15436==
                 by 0x489AFF: Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x489549: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                 ==15436==
==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) ==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436== Invalid read of size 2
                 at 0x431C95: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                 by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                 by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4884FD: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                 by 0x489825: Parser::get0bj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                 by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, catalog*, int (*)(void*), void*) (in
==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 by 0x42ECBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436== Address 0x5b100bc is 0 bytes after a block of size 108 alloc'd
==15436==
                 at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==15436==
                 by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x43051F: CCITFaxStream::CCITFaxStream(Stream*, int, int, int, int, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
==15436==
                 by 0x42CE76: Stream::makeFilter(char*, Stream*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x42C6AF: Stream::addFilters(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 by 0x489AFF: Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489549: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                 by 0x43FA44: XRef::fetch(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 by 0x4284A9: Object::fetch(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==15436==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== Invalid read of size 2
                 at 0x431CBF: CCITTFaxStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 by 0x43ADDC: CCITTFaxStream::getChar() (in /home/dungnguyen/PoCs/pdf2json_6671b64/pdf2json) by 0x40947A: Object::streamGetChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                 by 0x48796F: Lexer::getChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
==15436==
                 by 0x4884FD: Lexer::get0bj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                 by 0x489825: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                 by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436==
                 by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) (in
==15436==
==15436==
/home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== bv 0x42BCBD: PDFDoc::displayPage(Out
                 by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==15436== Address 0x5b100bc is 0 bytes after a block of size 108 alloc'd
```

```
==15436==
                            at 0x4C2DB8F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
     ==15436==
                            by 0x48E521: gmalloc (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
    ==15436==
                            by 0x48E667: gmallocn (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x43E567: CCITTFaxStream::CCITTFaxStream(Stream*, int, int, int, int, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==15436==
                            by 0x42CE76: Stream::makeFilter(char*, Stream*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x42C6AF: Stream::addFilters(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==15436==
                            by 0x4894Ff: Parser::makeStream(Object*, unsigned char*, cryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489549: Parser::makeStream(Object*, unsigned char*, cryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x489549: Parser::getObj(Object*, unsigned char*, cryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4284A9: Object::fetCh(int, int, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x428A9: Object::fetCh(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x428A565: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) (in
    ==15436==
     ==15436==
     ==15436==
     ==15436==
==15436==
     /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                            by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
     ==15436==
     /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
      ==15436==
    Error: Unknown operator 'The Armon Street Control of the Control o
                            ==15436==
     /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) ==15436== by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
    /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                            by 0x428CBO1: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x428D48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==15436==
                             by 0x40269A: main (pdf2json.cc:275)
     ==15436== Address 0xfdccfdb8fdb30035 is not stack'd, malloc'd or (recently) free'd
     ==15436==
     ==15436==
     ==15436== Process terminating with default action of signal 11 (SIGSEGV)
     ==15436== General Protection Fault
                            at 0x41C7A2: GfxState::restore() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x467BEB: Gfx::restoreState() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==15436==
     ==15436== by 0x42A5AA: 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)
                            by 0x42A14A: Page::display(OutputDev*, double, double, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
     ==15436==
     /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                        by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
    ==15436==
                            by 0x428048: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                           by 0x40269A: main (pdf2json.cc:275)
     ==15436==
     ==15436==
     ==15436== HEAP SUMMARY:
     ==15436== in use at exit: 211,954 bytes in 1,760 blocks
==15436== total heap usage: 2,027 allocs, 267 frees, 304,086 bytes allocated
     ==15436==
     ==15436==
     ==15436== LEAK SUMMARY:
     ==15436== definitely lost: 760 bytes in 4 blocks
                         indirectly lost: 192 bytes in 5 blocks
     ==15436==
                                possibly lost: 0 bytes in 0 blocks
     ==15436== still reachable: 211,002 bytes in 1,751 blocks
     ==15436==
                                      suppressed: 0 bytes in 0 blocks
     ==15436== Rerun with --leak-check=full to see details of leaked memory
     ==15436==
    ==15436== For counts of detected and suppressed errors, rerun with: -v ==15436== ERROR SUMMARY: 483 errors from 15 contexts (suppressed: 0 from 0)
    Segmentation fault
Thanks,
Manh Dung
```

Assignees

No one assigned

Labels

None yet

Projects

rvone yet

No milestone

Developmen

No branches or pull requests

1 participant

