New issue

Jump to bottom

SEGV (use after free) on DCTStream::transformDataUnit #28

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 an Use After Free bug on the function DCTStream::transformDataUnit (the latest commit `b671b64` on master - version 0.70).

PoC: https://github.com/strongcourage/PoCs/blob/master/pdf2json_b671b64/PoC_uaf_DCTStream::transformDataUnit

Valgrind says:

```
pdf2json $PoC /dev/null
...
==12935== Invalid read of size 2
==12935==    at 0x436149: DCTStream::transformDataUnit(unsigned short*, int*, unsigned char*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x43363B: DCTStream::readMCURow() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4331D7: DCTStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4887E8: Object::streamLookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x487A5B: Lexer::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4884C8: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x489825: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4892BE: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    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)
==12935==  Address 0x5b21c10 is 16 bytes inside a block of size 32 free'd
==12935==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==12935==    by 0x428565: Object::free() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x446431: Array::~Array() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x42855D: Object::free() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x446431: Array::~Array() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x42855D: Object::free() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x446431: Array::~Array() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x42855D: Object::free() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x446431: Array::~Array() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x42855D: Object::free() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x446431: Array::~Array() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x42855D: Object::free() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==  Block was alloc'd at
==12935==    at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==12935==    by 0x428284: Object::initArray(XRef*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x48924E: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4892BE: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4892BE: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4892BE: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4892BE: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4892BE: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4892BE: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    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)
==12935==
==12935== Invalid read of size 1
==12935==    at 0x43698B: DCTStream::transformDataUnit(unsigned short*, int*, unsigned char*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x43363B: DCTStream::readMCURow() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4331D7: DCTStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4887E8: Object::streamLookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x487A5B: Lexer::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4884C8: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x489825: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4892BE: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    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)
==12935==  Address 0x6ff09c is not stack'd, malloc'd or (recently) free'd
==12935==
==12935==
==12935== Process terminating with default action of signal 11 (SIGSEGV)
==12935==  Access not within mapped region at address 0x6FF09C
==12935==    at 0x43698B: DCTStream::transformDataUnit(unsigned short*, int*, unsigned char*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x43363B: DCTStream::readMCURow() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4331D7: DCTStream::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4887E8: Object::streamLookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x487A5B: Lexer::lookChar() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4884C8: Lexer::getObj(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x489C19: Parser::shift() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x489825: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x4892BE: Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x454759: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==12935==    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)
==12935==  If you believe this happened as a result of a stack
==12935==  overflow in your program's main thread (unlikely but
==12935==  possible), you can try to increase the size of the
==12935==  main thread stack using the --main-stacksize= flag.
==12935==  The main thread stack size used in this run was 8388608.
==12935==
==12935== HEAP SUMMARY:
==12935==     in use at exit: 227,902 bytes in 1,796 blocks
==12935==   total heap usage: 2,505 allocs, 709 frees, 362,560 bytes allocated
```

```
==12935==
==12935== LEAK SUMMARY:
==12935==    definitely lost: 16 bytes in 1 blocks
==12935==    indirectly lost: 8 bytes in 1 blocks
==12935==      possibly lost: 0 bytes in 0 blocks
==12935==    still reachable: 227,878 bytes in 1,794 blocks
==12935==         suppressed: 0 bytes in 0 blocks
==12935== Rerun with --leak-check=full to see details of leaked memory
==12935==
==12935== For counts of detected and suppressed errors, rerun with: -v
==12935== ERROR SUMMARY: 1921 errors from 3 contexts (suppressed: 0 from 0)
Segmentation fault
```

Thanks,
Manh Dung

strongcourage changed the title ~~Segmentation fault (use after free) on DCTStream::transformDataUnit~~ **SEGV (use after free) on DCTStream::transformDataUnit** 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