New issue

Jump to bottom

Invalid read on DCTStream::readHuffSym #33

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::readHuffSym (the latest commit `b671b64` on master - version 0.70).

PoC: https://github.com/strongcourage/PoCs/blob/master/pdf2json_b671b64/PoC_ir_DCTStream::readHuffSym

Valgrind says:

```
valgrind pdf2json $PoC /dev/null
==8920== Memcheck, a memory error detector
==8920== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
==8920== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
==8920== Command: ./pdf2json ./PoC_ir_DCTStream::readHuffSym /dev/null
==8920==
Error: PDF file is damaged - attempting to reconstruct xref table...
Error (17141): Illegal character <5c> in hex string
Error (17152): Illegal character <78> in hex string
Error (105): Dictionary key must be a name object
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 (8143): Command token too long
Error (8143): Missing 'endstream'
==8920== Invalid read of size 2
==8920==    at 0x436A05: DCTStream::readHuffSym(DCTHuffTable*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x434C67: DCTStream::readProgressiveDataUnit(DCTHuffTable*, DCTHuffTable*, int*, int*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x434765: DCTStream::readScan() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x432C49: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    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)
==8920==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x40269A: main (pdf2json.cc:275)
==8920==  Address 0x5b124e2 is 2 bytes after a block of size 32 alloc'd
==8920==    at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==8920==    by 0x4877C8: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    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)
==8920==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x40269A: main (pdf2json.cc:275)
==8920==
==8920== Invalid read of size 2
==8920==    at 0x436A1F: DCTStream::readHuffSym(DCTHuffTable*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x434C67: DCTStream::readProgressiveDataUnit(DCTHuffTable*, DCTHuffTable*, int*, int*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x434765: DCTStream::readScan() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x432C49: DCTStream::reset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x40941E: Object::streamReset() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x48788A: Lexer::Lexer(XRef*, Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x4542CE: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    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)
==8920==    by 0x42A14A: Page::display(OutputDev*, double, double, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x42BCBD: PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x42BD48: PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==8920==    by 0x40269A: main (pdf2json.cc:275)
==8920==  Address 0x5b12504 is 28 bytes before a block of size 128 in arena "client"
==8920==
Error (1759): Bad Huffman code in DCT stream
Error (12887): Bad DCT header
Error (12887): Unknown operator
'<long run of replacement characters>'
...
==8920==
==8920== HEAP SUMMARY:
==8920==     in use at exit: 72,744 bytes in 4 blocks
==8920==   total heap usage: 2,947 allocs, 2,943 frees, 693,136 bytes allocated
==8920==
==8920== LEAK SUMMARY:
==8920==    definitely lost: 32 bytes in 2 blocks
==8920==    indirectly lost: 8 bytes in 1 blocks
==8920==      possibly lost: 0 bytes in 0 blocks
==8920==    still reachable: 72,704 bytes in 1 blocks
==8920==         suppressed: 0 bytes in 0 blocks
==8920== Rerun with --leak-check=full to see details of leaked memory
==8920==
==8920== For counts of detected and suppressed errors, rerun with: -v
==8920== ERROR SUMMARY: 30 errors from 2 contexts (suppressed: 0 from 0)
```

Thanks,
Manh Dung

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant