

Summary

There is an "allocator is out of memory" vulnerability in qpdf-11.9.1(<https://github.com/qpdf/qpdf/releases/tag/v11.9.1>).

Affected component is `--pages` option.

Details

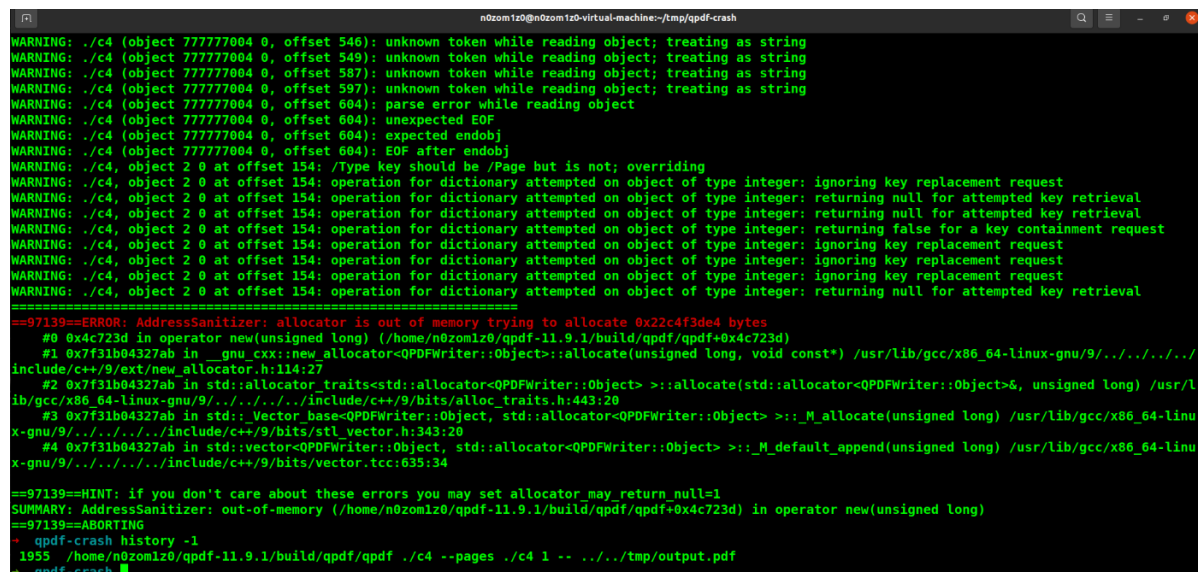
Build from source code with afl-clang-fast and ASAN enabled:

```
cmake -DCMAKE_C_COMPILER=afl-clang-fast -DCMAKE_CXX_COMPILER=afl-clang-fast++ -S
. -B build -DCMAKE_BUILD_TYPE=RelWithDebInfo
cmake -DCMAKE_C_COMPILER=afl-clang-fast -DCMAKE_CXX_COMPILER=afl-clang-fast++ --
build build
AFL_USE_ASAN=1 make
```

When use `--pages` options with a crafted pdf file:

```
/home/n0zom1z0/qpdf-11.9.1/build/qpdf/qpdf ./c4 --pages ./c4 1 --
../tmp/output.pdf
```

error occurs:



```
n0zom1z0@n0zom1z0-virtual-machine:~/tmp/qpdf-crash
WARNING: ./c4 (object 777777004 0, offset 546): unknown token while reading object; treating as string
WARNING: ./c4 (object 777777004 0, offset 549): unknown token while reading object; treating as string
WARNING: ./c4 (object 777777004 0, offset 587): unknown token while reading object; treating as string
WARNING: ./c4 (object 777777004 0, offset 597): unknown token while reading object; treating as string
WARNING: ./c4 (object 777777004 0, offset 604): parse error while reading object
WARNING: ./c4 (object 777777004 0, offset 604): unexpected EOF
WARNING: ./c4 (object 777777004 0, offset 604): expected endobj
WARNING: ./c4 (object 777777004 0, offset 604): EOF after endobj
WARNING: ./c4, object 2 0 at offset 154: /Type key should be /Page but is not; overriding
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: ignoring key replacement request
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: returning null for attempted key retrieval
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: returning null for attempted key retrieval
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: returning false for a key containment request
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: ignoring key replacement request
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: ignoring key replacement request
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: ignoring key replacement request
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: returning null for attempted key retrieval
=====
==97139==ERROR: AddressSanitizer: allocator is out of memory trying to allocate 0x22c4f3de4 bytes
#0 0x4c723d in operator new(unsigned long) (/home/n0zom1z0/qpdf-11.9.1/build/qpdf/qpdf+0x4c723d)
#1 0x7f31b04327ab in __gnu_cxx::new_allocator<QPDFWriter::Object>::allocate(unsigned long, void const*) /usr/lib/gcc/x86_64-linux-gnu/9/../../../../
include/c++/9/ext/new_allocator.h:114:27
#2 0x7f31b04327ab in std::allocator_traits<std::allocator<QPDFWriter::Object> >::allocate(std::allocator<QPDFWriter::Object> &, unsigned long) /usr/l
ib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/alloc_traits.h:443:20
#3 0x7f31b04327ab in std::_Vector_base<QPDFWriter::Object, std::allocator<QPDFWriter::Object> >::_M_allocate(unsigned long) /usr/lib/gcc/x86_64-linu
x-gnu/9/../../../../include/c++/9/bits/stl_vector.h:343:20
#4 0x7f31b04327ab in std::_vector<QPDFWriter::Object, std::allocator<QPDFWriter::Object> >::_M_default_append(unsigned long) /usr/lib/gcc/x86_64-linu
x-gnu/9/../../../../include/c++/9/bits/vector.tcc:635:34
==97139==HINT: if you don't care about these errors you may set allocator may return null=1
SUMMARY: AddressSanitizer: out-of-memory (/home/n0zom1z0/qpdf-11.9.1/build/qpdf/qpdf+0x4c723d) in operator new(unsigned long)
==97139==ABORTING
+ qpdf-crash history -1
1953 /home/n0zom1z0/qpdf-11.9.1/build/qpdf/qpdf ./c4 --pages ./c4 1 -- ../tmp/output.pdf
+ qpdf-crash
```

And I upload this crafted pdf file here: <https://drive.google.com/drive/folders/1CrWh5kDE6nFCdyeGtXnFQSQZj19xeUwn?usp=sharing>

PoC

c4: <https://drive.google.com/drive/folders/1CrWh5kDE6nFCdyeGtXnFQSQZj19xeUwn?usp=sharing>

```
/home/n0zom1z0/qpdf-11.9.1/build/qpdf/qpdf ./c4 --pages ./c4 1 --  
../tmp/output.pdf
```

```
n0zom1z0@n0zom1z0-virtual-machine:~/tmp/qpdf-crash
WARNING: ./c4 (object 777777004 0, offset 546): unknown token while reading object; treating as string
WARNING: ./c4 (object 777777004 0, offset 549): unknown token while reading object; treating as string
WARNING: ./c4 (object 777777004 0, offset 587): unknown token while reading object; treating as string
WARNING: ./c4 (object 777777004 0, offset 587): unknown token while reading object; treating as string
WARNING: ./c4 (object 777777004 0, offset 604): parse error while reading object
WARNING: ./c4 (object 777777004 0, offset 604): unexpected EOF
WARNING: ./c4 (object 777777004 0, offset 604): expected endobj
WARNING: ./c4 (object 777777004 0, offset 604): EOF after endobj
WARNING: ./c4, object 2 0 at offset 154: /Type key should be /Page but is not; overriding
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: ignoring key replacement request
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: returning null for attempted key retrieval
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: returning null for attempted key retrieval
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: returning false for a key containment request
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: ignoring key replacement request
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: ignoring key replacement request
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: ignoring key replacement request
WARNING: ./c4, object 2 0 at offset 154: operation for dictionary attempted on object of type integer: returning null for attempted key retrieval
=====
==97139==ERROR: AddressSanitizer: allocator is out of memory trying to allocate 0x22c4f3de4 bytes
#0 0x4c723d in operator new(unsigned long) (/home/n0zom1z0/qpdf-11.9.1/build/qpdf/qpdf+0x4c723d)
#1 0x7f31b04327ab in __gnu_cxx::new_allocator<QPDFWriter::Object>::allocate(unsigned long, void const*) /usr/lib/gcc/x86_64-linux-gnu/9/../../../../lib/c++/9/ext/new_allocator.h:114:27
#2 0x7f31b04327ab in std::allocator_traits<std::allocator<QPDFWriter::Object> >::allocate(std::allocator<QPDFWriter::Object> &, unsigned long) /usr/lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/alloc_traits.h:443:20
#3 0x7f31b04327ab in std::vector base<QPDFWriter::Object, std::allocator<QPDFWriter::Object> >::_M_allocate(unsigned long) /usr/lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/stl_vector.h:343:20
#4 0x7f31b04327ab in std::vector<QPDFWriter::Object, std::allocator<QPDFWriter::Object> >::_M_default_append(unsigned long) /usr/lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/vector.tcc:635:34
==97139==HINT: if you don't care about these errors you may set allocator may return null=1
SUMMARY: AddressSanitizer: out-of-memory (/home/n0zom1z0/qpdf-11.9.1/build/qpdf/qpdf+0x4c723d) in operator new(unsigned long)
==97139==ABORTING
+ qpdf-crash history -1
1955 /home/n0zom1z0/qpdf-11.9.1/build/qpdf/qpdf ./c4 --pages ./c4 1 -- ../tmp/output.pdf
+ qpdf-crash
```