

# 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 `--decrypt` option.

## Details

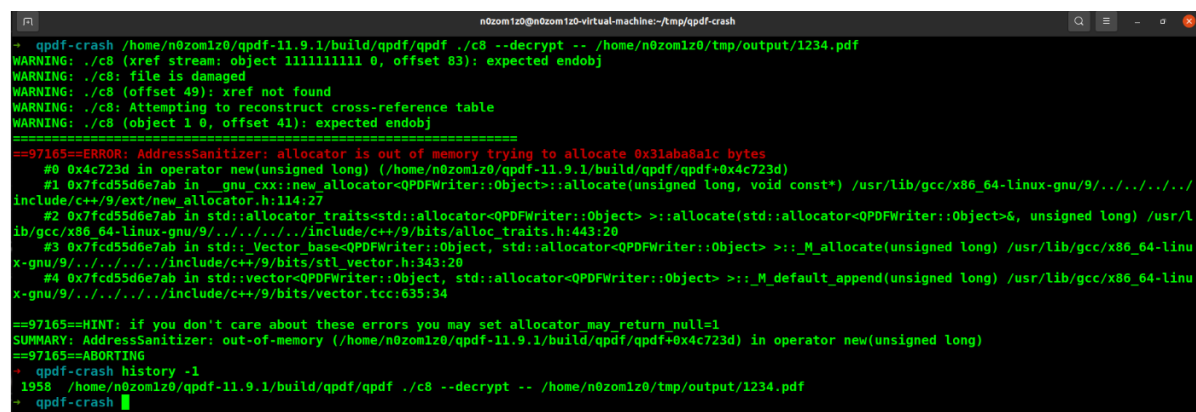
Build from source code with afl-clang-fast and ASAN enabled:

```
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 `--decrypt` options with a crafted pdf file:

```
/home/n0z0mlz0/qpdf-11.9.1/build/qpdf/qpdf ./c8 --decrypt --
/home/n0z0mlz0/tmp/output/1234.pdf
```

error occurs:



```
+ qpdf-crash /home/n0z0mlz0/qpdf-11.9.1/build/qpdf/qpdf ./c8 --decrypt -- /home/n0z0mlz0/tmp/output/1234.pdf
WARNING: ./c8 (xref stream: object 111111111 0, offset 83): expected endobj
WARNING: ./c8: file is damaged
WARNING: ./c8 (offset 49): xref not found
WARNING: ./c8: Attempting to reconstruct cross-reference table
WARNING: ./c8 (object 1 0, offset 41): expected endobj
=====
==97165==ERROR: AddressSanitizer: allocator is out of memory trying to allocate 0x31aba8a1c bytes
#0 0x4c723d in operator new(unsigned long) (/home/n0z0mlz0/qpdf-11.9.1/build/qpdf/qpdf+0x4c723d)
#1 0x7fcd55d6e7ab 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 0x7fcd55d6e7ab 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 0x7fcd55d6e7ab 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 0x7fcd55d6e7ab 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
==97165==HINT: if you don't care about these errors you may set allocator_null=1
SUMMARY: AddressSanitizer: out-of-memory (/home/n0z0mlz0/qpdf-11.9.1/build/qpdf/qpdf+0x4c723d) in operator new(unsigned long)
==97165==ABORTING
+ qpdf-crash history -1
1958 /home/n0z0mlz0/qpdf-11.9.1/build/qpdf/qpdf ./c8 --decrypt -- /home/n0z0mlz0/tmp/output/1234.pdf
+ qpdf-crash
```

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

## PoC

c8: <https://drive.google.com/drive/folders/1CrWh5kDE6nFCdyeGtXnFQSQZj19xeUwn?usp=sharing>  
g

```
/home/n0zom1z0/qpdf-11.9.1/build/qpdf/qpdf ./c8 --decrypt --  
/home/n0zom1z0/tmp/output/1234.pdf
```