

heap-buffer-overflow in pdftoppm at XRef.cc:607 in XRef::readXRefTable

Post Reply 

Search this topic...




2 posts • Page 1 of 1

verf1sh



heap-buffer-overflow in pdftoppm at XRef.cc:607 in XRef::readXRefTable

 Mon Dec 06, 2021 12:54 pm

Hello,

We are currently working on fuzz testing feature, and we found a **heap buffer overflow** in the function readXRefTable located in XRef.cc. It can be triggered by sending a crafted PDF file to the **pdftoppm(version 4.0.3)** binary.

The stack traces are as follow:

CODE: SELECT ALL

```
==2823306==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6290000051b0 at pc 0x55f052e601
READ of size 8 at 0x6290000051b0 thread T0
#0 0x55f052e601f6 in XRef::readXRefTable(long*, int, XRefPosSet*) /root/fuzz/fuzzing101/exercisel
#1 0x55f052e5cee3 in XRef::readXRef(long*, XRefPosSet*, int) /root/fuzz/fuzzing101/exercisel/fuzz
#2 0x55f052e71076 in XRef::XRef(BaseStream*, int) /root/fuzz/fuzzing101/exercisel/fuzzing_xpdf/xp
#3 0x55f052dd1465 in PDFDoc::setup2(GString*, GString*, int) /root/fuzz/fuzzing101/exercisel/fuzz
#4 0x55f052dd1d8d in PDFDoc::setup(GString*, GString*) /root/fuzz/fuzzing101/exercisel/fuzzing_xp
#5 0x55f052dd322b in PDFDoc::PDFDoc(char*, GString*, GString*, PDFCore*) /root/fuzz/fuzzing101/ex
#6 0x55f052a56531 in main /root/fuzz/fuzzing101/exercisel/fuzzing_xpdf/xpdf-4.03/xpdf/pdftoppm.cc
#7 0x7f0b14b290b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
#8 0x55f052a5927d in _start (/root/fuzz/fuzzing101/exercisel/fuzzing_xpdf/xpdf-4.03/build2/xpdf/p
0x6290000051b0 is located 80 bytes to the left of 16384-byte region [0x629000005200,0x629000009200)
```

You can reproduce this bug by the follow step:

CODE: SELECT ALL

```
mkdir build
cd build
export CC=afl-clang-fast
export CXX=afl-clang-fast++
cmake ..
AFL_USE_ASAN=1 make -j8
./pdftoppm ./poc_ppm 3.ppm
```

You can download this PoC file at **ATTACHMENTS**

Environment

- Tested on Ubuntu 20.04.3 LTS x86_64, AFL++
- gcc version 10.3.0
- xpdf version: [xpdf 4.3.0](<https://dl.xpdfreader.com/xpdf-4.03.tar.gz>)

Thank you.

ATTACHMENTS

[poc_ppm.zip](#)

(143.69 KiB) Downloaded 124 times



derekn



Re: heap-buffer-overflow in pdftoppm at XRef.cc:607 in XRef::readXRefTable

Mon Dec 06, 2021 10:14 pm

This turned out to be the same bug as [viewtopic.php?f=3&t=42197](#)

Thanks for the report.



Post Reply



2 posts • Page **1** of **1**

[Return to "Xpdf open source"](#)

Jump to



[Board index](#)

Delete cookies All times are UTC