PDFunite 0.41.0 - '.pdf' Local Buffer Overflow

EDB-ID:
44490

CVE:
N/A

EDB Verified: ×

Author:
HAMM3R.PY

Type:
DOS

Exploit: / {}

Platform:
LINUX

Date:
2018-04-18

Vulnerable App:

```
# Exploit Title: PDFunite Malformed pdf buffer overflow
# Date: 17 April 2018
# Exploit Author: Hamm3r.py
# Vendor Homepage: https://launchpad.net/ubuntu/artful/+package/poppler-
utils
# Software Link: https://launchpad.net/ubuntu/+source/poppler/0.57.0-
2ubuntu4.2
# Version: 0.41.0
# Tested on: Ubuntu
# CVE :

pdfunite is a part of poppler package in ubuntu. pdfunite is prone to a
local bufferoverflow when a malformed pdf is used to unite with another
pdf.
Following is the gdb stack trace:

Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff7abf948 in XRef::getEntry(int, bool) () from
/usr/lib/x86_64-linux-gnu/libpoppler.so.58
#0 0x00007ffff7abf948 in XRef::getEntry(int, bool) () from
/usr/lib/x86_64-linux-gnu/libpoppler.so.58
#1 0x00007ffff7aa8867 in PDFDoc::markObject(Object*, XRef*, XRef*,
unsigned int, int, int, std::set<Dict*, std::less<Dict*>,
std::allocator<Dict*> >*) () from /usr/lib/x86_64-linux-
gnu/libpoppler.so.58
#2 0x00007ffff7aa85a3 in PDFDoc::markDictionnary(Dict*, XRef*, XRef*,
unsigned int, int, int, std::set<Dict*, std::less<Dict*>,
std::allocator<Dict*> >*) () from /usr/lib/x86_64-linux-
gnu/libpoppler.so.58
#3 0x00007ffff7aa884c in PDFDoc::markObject(Object*, XRef*, XRef*,
unsigned int, int, int, std::set<Dict*, std::less<Dict*>,
std::allocator<Dict*> >*) () from /usr/lib/x86_64-linux-
gnu/libpoppler.so.58
#4 0x00007ffff7aa8971 in PDFDoc::markObject(Object*, XRef*, XRef*,
unsigned int, int, int, std::set<Dict*, std::less<Dict*>,
std::allocator<Dict*> >*) () from /usr/lib/x86_64-linux-
gnu/libpoppler.so.58
#5 0x00007ffff7aa85a3 in PDFDoc::markDictionnary(Dict*, XRef*, XRef*,
unsigned int, int, int, std::set<Dict*, std::less<Dict*>,
std::allocator<Dict*> >*) () from /usr/lib/x86_64-linux-
gnu/libpoppler.so.58
#6 0x00007ffff7aa884c in PDFDoc::markObject(Object*, XRef*, XRef*,
unsigned int, int, int, std::set<Dict*, std::less<Dict*>,
std::allocator<Dict*> >*) () from /usr/lib/x86_64-linux-
gnu/libpoppler.so.58
#7 0x00007ffff7aa8971 in PDFDoc::markObject(Object*, XRef*, XRef*,
unsigned int, int, int, std::set<Dict*, std::less<Dict*>,
std::allocator<Dict*> >*) () from /usr/lib/x86_64-linux-
gnu/libpoppler.so.58
#8 0x00007ffff7aa85a3 in PDFDoc::markDictionnary(Dict*, XRef*, XRef*,
unsigned int, int, int, std::set<Dict*, std::less<Dict*>,
std::allocator<Dict*> >*) () from /usr/lib/x86_64-linux-
gnu/libpoppler.so.58
#9 0x00007ffff7aa884c in PDFDoc::markObject(Object*, XRef*, XRef*,
unsigned int, int, int, std::set<Dict*, std::less<Dict*>,
std::allocator<Dict*> >*) () from /usr/lib/x86_64-linux-
gnu/libpoppler.so.58
#10 0x00007ffff7aa8bae in PDFDoc::markPageObjects(Dict*, XRef*, XRef*,
unsigned int, int, int, std::set<Dict*, std::less<Dict*>,
std::allocator<Dict*> >*) () from /usr/lib/x86_64-linux-
gnu/libpoppler.so.58
#11 0x000000000040271a in ?? ()
#12 0x00007ffff722d830 in __libc_start_main (main=0x401b20, argc=4,
argv=0x7fffffffe0b8, init=<optimized out>, fini=<optimized out>,
rtld_fini=<optimized out>, stack_end=0x7fffffffe0a8) at
```

```
../csu/libc-start.c:291
#13 0x0000000000403179 in ?? ()


$ pdfunite -v
pdfunite version 0.41.0


#This issue is identified by Hamm3r.py, a general purpose fuzzer!


Proof of Concept:
https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-
sploits/44490.zip
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions