stack-overflow by Xpdf4.04

Post Reply Search this topic... 3 posts • Page 1 of 1

bugchong

stack-overflow by Xpdf4.04

Fri Aug 05, 2022 7:02 am

hi,i use AFL++ fuzz xpdf4.04,and found the Catalog::countPageTree() function in Catalog.cc may cause recursion issues via a crafted file.

CODE: SELECT ALL

```
gdb --args pdftopng crashfile output/
```

CODE: SELECT ALL

```
Syntax Error (1262): Dictionary key must be a name object
Syntax Error (1265): Dictionary key must be a name object

Program received signal SIGSEGV, Segmentation fault.

[----------------------------------registers-----------------------------------]
RAX: 0x5f8fd980549df300
RBX: 0x7fffff7ff050 --> 0x7fffff7ff060 --> 0x7ffff6ef6b41 (<malloc+193>:        mov    r15,rax)
RCX: 0x7fffff7ff000 --> 0x0
RDX: 0x7fffff7ff8a0 --> 0xfffffffffffffff90
RSI: 0x7fffff7ff050 --> 0x7fffff7ff060 --> 0x7ffff6ef6b41 (<malloc+193>:        mov    r15,rax)
RDI: 0x7
RBP: 0x7fffff7ff050 --> 0x7fffff7ff060 --> 0x7ffff6ef6b41 (<malloc+193>:        mov    r15,rax)
RSP: 0x7fffff7fefe0
```

bt

CODE: SELECT ALL

```
#29095 0x000055555577c369 in Catalog::countPageTree (this=this@entry=0x612000000040, pagesObj=pagesOb
#29096 0x000055555577c369 in Catalog::countPageTree (this=this@entry=0x612000000040, pagesObj=pagesOb
#29097 0x000055555577c369 in Catalog::countPageTree (this=this@entry=0x612000000040, pagesObj=pagesOb
#29098 0x000055555577c369 in Catalog::countPageTree (this=this@entry=0x612000000040, pagesObj=pagesOb
#29099 0x000055555577c369 in Catalog::countPageTree (this=this@entry=0x612000000040, pagesObj=pagesOb
#29100 0x000055555577c369 in Catalog::countPageTree (this=this@entry=0x612000000040, pagesObj=pagesOb
#29101 0x000055555577c369 in Catalog::countPageTree (this=this@entry=0x612000000040, pagesObj=pagesOb
#29102 0x000055555577c369 in Catalog::countPageTree (this=this@entry=0x612000000040, pagesObj=pagesOb
#29103 0x000055555577c369 in Catalog::countPageTree (this=this@entry=0x612000000040, pagesObj=pagesOb
#29104 0x000055555577c369 in Catalog::countPageTree (this=this@entry=0x612000000040, pagesObj=pagesOb
#29105 0x000055555577d9a8 in Catalog::readPageTree (this=this@entry=0x612000000040, catDict=catDict@e
#29106 0x0000555555789d11 in Catalog::Catalog (this=0x612000000040, docA=<optimized out>) at /home/he
#29107 0x0000555555a6141e in PDFDoc::setup2 (this=this@entry=0x607000000090, ownerPassword=ownerPassw
```

please check it out,thanks

ATTACHMENTS

crash.zip
(1.08 KiB) Downloaded 194 times

derekn

Re: stack-overflow by Xpdf4.04

Thu Aug 11, 2022 11:27 pm

That's an object loop in the PDF file. I'm working on a more robust loop detector for Xpdf 5.

bugchong

Re: stack-overflow by Xpdf4.04

Fri Aug 12, 2022 9:10 am

> **derekn wrote:** ↑
> That's an object loop in the PDF file. I'm working on a more robust loop detector for Xpdf 5.

OK.Thanks.

Post Reply

3 posts • Page **1** of **1**

‹ Return to "Xpdf open source"

Jump to

Board index

Delete cookies All times are UTC