A SEGV in TextString.cc:47 in xpdf-4.02

b166er_fauxre

A SEGV in TextString.cc:47 in xpdf-4.02

Wed Aug 26, 2020 8:39 am

Version: xpdf-4.02

OS: Ubuntu 16.04 LTS

cmd: ./pdftohtml -r 300 POC /dev/null

Abstract: Fuzzing pdftohtml the target binary crashes due to an access violation

Log:

Program received signal SIGSEGV, Segmentation fault.
TextString::~TextString (this=0x21, __in_chrg=<optimized out>) at /home/b166er/xpdf-4.02/xpdf/TextString.cc:47
47 gfree(u);
(gdb) backtrace
#0 TextString::~TextString (this=0x21, __in_chrg=<optimized out>) at /home/b166er/xpdf-4.02/xpdf/TextString.cc:47
#1 0x00000000004750c2 in PageLabelNode::~PageLabelNode (this=<optimized out>, __in_chrg=<optimized out>) at /home/b166er/xpdf-4.02/xpdf/Catalog.cc:141
#2 0x0000000000475264 in Catalog::~Catalog (this=0x81dad0, __in_chrg=<optimized out>) at /home/b166er/xpdf-4.02/xpdf/Catalog.cc:295
#3 0x00000000004e02d3 in PDFDoc::setup2 (this=this@entry=0x81a7c0, ownerPassword=ownerPassword@entry=0x0, userPassword=userPassword@entry=0x0, repairXRef=repairXRef@entry=1) at /home/b166er/xpdf-4.02/xpdf/PDFDoc.cc:312
#4 0x00000000004e03a2 in PDFDoc::setup (this=this@entry=0x81a7c0, ownerPassword=ownerPassword@entry=0x0, userPassword=userPassword@entry=0x0) at /home/b166er/xpdf-4.02/xpdf/PDFDoc.cc:266
#5 0x00000000004e0657 in PDFDoc::PDFDoc (this=0x81a7c0, fileNameA=0x7fffffffe84e "/home/b166er/127.pdf", ownerPassword=0x0, userPassword=0x0, coreA=<optimized out>) at /home/b166er/xpdf-4.02/xpdf/PDFDoc.cc:208
#6 0x00000000004476ad in main (argc=3, argv=0x7fffffffe5e8) at /home/b166er/xpdf-4.02/xpdf/pdftohtml.cc:129

Catalog.cc Line:141 When deconstruct PageLabelNode as follow:

PageLabelNode::~PageLabelNode() {
delete prefix;
}
gdb shows that prefix is invalid address:

Breakpoint 45, PDFDoc::setup2 (this=this@entry=0x81a7c0, ownerPassword=ownerPassword@entry=0x0, userPassword=userPassword@entry=0x0, repairXRef=repairXRef@entry=1) at /home/b166er/xpdf-4.02/xpdf/PDFDoc.cc:312
312 delete catalog;

Breakpoint 21, Catalog::~Catalog (this=0x81dad0, __in_chrg=<optimized out>) at /home/b166er/xpdf-4.02/xpdf/Catalog.cc:295
295 deleteGList(pageLabels, PageLabelNode);

Breakpoint 22, GList::get (this=0x7ffff6e37b98, i=0) at /home/b166er/xpdf-4.02/goo/GList.h:48
48 void *get(int i) { return data; }

Breakpoint 28, PageLabelNode::~PageLabelNode (this=0x81dc70, __in_chrg=<optimized out>) at /home/b166er/xpdf-4.02/xpdf/Catalog.cc:141
141 delete prefix;
(gdb) p prefix
*$1 = (TextString *) 0x21*
(gdb) x/16x $1
0x21: Cannot access memory at address 0x21

*It seems to be TextString *prefix in PageLabelNode class(Catalog.cc Line:103) without being initialized properly. As a result, TextString.cc Line:47*

TextString::~TextString() {
gfree(u);
}
free a invalid memory address.

Please see the testcase sample in attachment.

Thanks.

ATTACHMENTS

testcase_cause_SEGV.zip
(976 Bytes) Downloaded 280 times

derekn

Re: A SEGV in TextString.cc:47 in xpdf-4.02

Thu Aug 27, 2020 6:37 pm

This is the same problem with Catalog.pageLabels not being initialized correctly.
(See viewtopic.php?f=3&t=41890.)