



PoDoFo Tickets

A PDF parsing, modification and creation library.
Brought to you by: domseichter

#48 stack buffer overflow at src/base/PdfDictionary.cpp:65 caused by excessive recursion in a PdfOutlineItem constructor



Milestone: [SVN](#)

Status: open

Owner: nobody

Labels: [security \(37\)](#)

[TRUNK](#)

Updated: 2022-05-04

Created: 2019-04-04

Creator: [Tao](#)

Private: No

Hi, there is a `stack buffer overflow` at `src/base/PdfDictionary.cpp:65`.
Poc is attach below.
the stack trace is shown following:

```
$ ./podofopdfinfo poc
Document Info
-----
File: unique-crashes/id:000028,sig:11,src:000039,op:flip1,pos:4920
PDF Version: 1.7
Page Count: 1
Page Size: 500 x 500 pts

Fast Web View Enabled: No
Tagged: No
Encrypted: No
Printing Allowed: Yes
Modification Allowed: Yes
Copy&Paste Allowed: Yes
Add/Modify Annotations Allowed: Yes
Fill&Sign Allowed: Yes
Accessibility Allowed: Yes
Document Assembly Allowed: Yes
High Quality Print Allowed: Yes

Classic Metadata
-----
Author:
Creator:
Subject:
Title:
Keywords:
Trapped:

Page Info
-----
Page Count: 1
Page 0:
->Internal Number:1
->Object Number:14 0 R
MediaBox: [ 0.000000 0.000000 500.000000 500.000000 ]
Rotation: 0
# of Annotations: 1

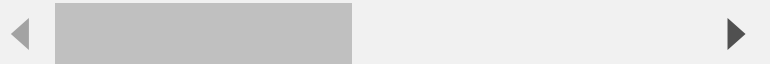
Annotation 0
Type: 19
Contents:
Title: Button
Flags: 4
Rect: [ 31.937100 416.754000 86.910800 469.634000 ]
Open: false

Outlines
-----
==111394==ERROR: AddressSanitizer: stack-overflow on address 0x7ffc3b485ef8 (pc 0x00000056d
#0 0x56d625 in __asan_memcpy /home/wdw/llvm-4.0.0.src/build/./projects/compiler-rt/lib
#1 0x5cd252 in PoDoFo::PdfDictionary::operator=(PoDoFo::PdfDictionary const&) /home/lt/
#2 0x5ccfd5 in PoDoFo::PdfDictionary::PdfDictionary(PoDoFo::PdfDictionary const&) /home
#3 0x61e2e2 in PoDoFo::PdfVariant::PdfVariant(PoDoFo::PdfDictionary const&) /home/lt/vu
#4 0x5eb854 in PoDoFo::PdfObject::PdfObject(PoDoFo::PdfReference const&, char const*) /l
#5 0x62511c in PoDoFo::PdfVecObjects::GetObject(PoDoFo::PdfReference const&) const /hom
#6 0x6cf921 in PoDoFo::PdfOutlineItem::PdfOutlineItem(PoDoFo::PdfObject*, PoDoFo::PdfO

....

#245 0x6cf970 in PoDoFo::PdfOutlineItem::PdfOutlineItem(PoDoFo::PdfObject*, PoDoFo::Pdf
#246 0x6cf970 in PoDoFo::PdfOutlineItem::PdfOutlineItem(PoDoFo::PdfObject*, PoDoFo::Pdf
#247 0x6cf970 in PoDoFo::PdfOutlineItem::PdfOutlineItem(PoDoFo::PdfObject*, PoDoFo::Pdf
#248 0x6cf970 in PoDoFo::PdfOutlineItem::PdfOutlineItem(PoDoFo::PdfObject*, PoDoFo::Pdf
#249 0x6cf970 in PoDoFo::PdfOutlineItem::PdfOutlineItem(PoDoFo::PdfObject*, PoDoFo::Pdf
#250 0x6cf970 in PoDoFo::PdfOutlineItem::PdfOutlineItem(PoDoFo::PdfObject*, PoDoFo::Pdf

SUMMARY: AddressSanitizer: stack-overflow /home/wdw/llvm-4.0.0.src/build/./projects/compile
==111394==ABORTING
```



1 Attachments

[stack-overflow-ticket-48](#)

Discussion



Matthew Brincke - 2019-05-08



- labels: --> security
- summary: stack buffer overflow at src/base/PdfDictionary.cpp:65 --> stack buffer overflow at src/base/PdfDictionary.cpp:65 caused by excessive recursion in a PdfOutlineItem constructor



Matthew Brincke - 2019-05-26



As the constructor `PoDoFo::PdfOutlineItem::PdfOutlineItem(PoDoFo::PdfObject*, PoDoFo::PdfOutlineItem*, PoDoFo::PdfOutlineItem*)` is the culprit also in issue #25, this very much looks like a duplicate of that one. This has just two calls more in its backtrace before it was

SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

Team

SourceForge Headquarters

225 Broadway Suite 1600

San Diego, CA 92101

+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status

