



yjgo



Bug Report: pdftotext in Xpdf 4.04

Mon Oct 03, 2022 7:35 am

Hello.

I am a security researcher and I tried to explore fuzzing.

During fuzzing, I found several crashes in the pdftotext in Xpdf 4.04.

The crashes were caused by Catalog::countPageTree() and Catalog::readPageLabelTree2(Object*) functions.

I used the following command to reproduce the crashes.

```
CODE: SELECT ALL
pdftotext poc.pdf
```

The following is backtrace log by ASAN. Crash 1 in binary pdtotext (using Poc1)

```
Syntax Error: Couldn't read xref table

Syntax Warning: PDF file is damaged - attempting to reconstruct xref table...

Syntax Error (314): Dictionary key must be a name object

Syntax Error (316): Dictionary key must be a name object

Syntax Error (318): Dictionary key must be a name object

Syntax Error (321): Dictionary key must be a name object

Syntax Error (330): Dictionary key must be a name object

Syntax Error (332): Dictionary key must be a name object

Syntax Error (336): Dictionary key must be a name object

Syntax Error (339): Dictionary key must be a name object

Syntax Error (345): Dictionary key must be a name object

AddressSanitizer: DEADLYSIGNAL
```

Crash 2 in binary pdftotext (using Poc2)

```
CODE: SELECT ALL

Syntax Error: Couldn't read xref table

Syntax Warning: PDF file is damaged - attempting to reconstruct xref table...

Syntax Error (5797): Dictionary key must be a name object

Syntax Error (5804): Dictionary key must be a name object

Syntax Error (6264): Illegal character ')'

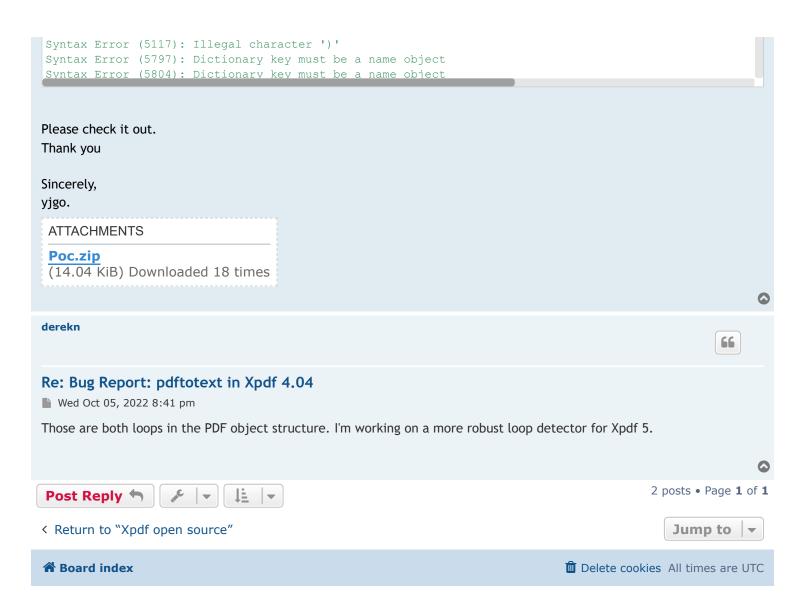
Syntax Error (6282): Illegal character '>'

Syntax Error (8723): Missing 'endstream'

Syntax Error (582): Dictionary key must be a name object

Syntax Error (584): Dictionary key must be a name object

Syntax Error (592): Dictionary key must be a name object
```



Powered by phpBBForum Software © phpBB Limited Privacy | Terms