xpdf 4.03 bug in pdftops

Taolaw

xpdf 4.03 bug in pdftops

Fri Feb 19, 2021 11:49 am

A NULL pointer dereference in the GString::getCString function in GString.h in xpdf-4.03 dirrerent viewtopic.php?f=3&t=41241&p=41808&hilit ... ing#p41808.

CODE: SELECT ALL

```
./pdftops 'null_point.pdf'


Syntax Error (92917): Command token too long
Syntax Error (93045): Command token too long
Syntax Error (93173): Command token too long
Syntax Error: Couldn't read xref table
Syntax Warning: PDF file is damaged - attempting to reconstruct xref table...
AddressSanitizer:DEADLYSIGNAL
=================================================================
==15006==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x55780e688f11 bp 0x7fff1cac0d50 sp 0x7fff1cac0d40 T0)
==15006==The signal is caused by a READ memory access.
```

ATTACHMENTS

null_point.pdf.txt
(131.63 KiB) Downloaded 198 times

derekn

Re: xpdf 4.03 bug in pdftops

Fri Feb 19, 2021 9:09 pm

There was a missing null check in XFAScanner::scanNode(). I'll fix that in the next release.

Thanks for the bug report.