Bug 703791 - mutool draw crashes with a specific file

Status: RESOLVED FIXED
Alias: None
Product: MuPDF
Component: apps (show other bugs)
Version: master
Hardware: PC Linux
Importance: P4 major
Assignee: muPDF bugs
URL:
Keywords:
Depends on:
Blocks:

Reported: 2021-04-19 18:53 UTC by Xuwei Liu
Modified: 2021-10-30 08:12 UTC (History)
CC List: 2 users (show)
See Also:
Customer:
Word Size: ---

Attachments	
poc file (1.25 KB, text/plain) 2021-04-19 18:53 UTC, Xuwei Liu	Details
Add an attachment (proposed patch, testcase, etc.)	

Note
You need to log in before you can comment on or make changes to this bug.

Xuwei Liu 2021-04-19 18:53:00 UTC — Description

Created attachment 20930 [details]
poc file

An invalid write makes mutool crashes.

Reproduce:
./mutool draw poc.txt

Asan output:
```
==10021==ERROR: AddressSanitizer: SEGV on unknown address 0x00004b808071 (pc
0x7f29cf36d565 bp 0x7ffd3cb64d10 sp 0x7ffd3cb64cc0 T0)
==10021==The signal is caused by a WRITE memory access.
    #0 0x7f29cf36d564  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x26564)
    #1 0x7f29cf4257c2 in __interceptor_free (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xde7c2)
    #2 0x50cbc8
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x50cbc8)
    #3 0x4cf3d0
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x4cf3d0)
    #4 0x45ba09
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x45ba09)
    #5 0x492686
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x492686)
    #6 0x4849db
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x4849db)
    #7 0x46512a
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x46512a)
    #8 0x4e218c
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x4e218c)
    #9 0x41565b
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x41565b)
    #10 0x41724a
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x41724a)
    #11 0x41addb
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x41addb)
    #12 0x41b51a
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x41b51a)
    #13 0x41da42
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x41da42)
    #14 0x410319
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x410319)
    #15 0x7f29ce5ff83f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2083f)
    #16 0x4143e8
(/home/youwei/genpdf/product/mupdf/mupdf/exe_asan/release/mutool+0x4143e8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x26564)
==10021==ABORTING
```

Tor Andersson 2021-04-27 12:08:44 UTC — Comment 1

commit f5712c9949d026e4b891b25837edd2edc166151f
Author: Tor Andersson <tor.andersson@artifex.com>
Date: Tue Apr 20 14:46:48 2021 +0200

~~Bug 703791~~: Stay within hash table max key size in cached color converter.

Ken Sharp 2021-10-30 08:07:53 UTC — Comment 4

User disabled due to spam, spam comment marked private to make it invisible