heap-use-after-free in method SplashOutputDev::endType3Char

mike

heap-use-after-free in method SplashOutputDev::endType3Char

Fri Nov 22, 2019 3:40 am

Hi,
I'm Mike Zhang of Pangu Lab, I found a heap-use-after-free bug in xpdf code.

4.02 xpdf under Ubuntu 16.04.3 LTS

CODE: SELECT ALL

```
pdftoppm pocfile /tmp/out
```

`SplashOutputDev::endType3Char(GfxState *state) SplashOutputDev.cc:3079` is trying to use the freed `t3GlyphStack->cache`, which causes an `heap-use-after-free` problem.

a log from Mac os debug:

CODE: SELECT ALL

```
==66891==ERROR: AddressSanitizer: heap-use-after-free on address 0x60800000c578 at pc 0x000108f0b06b bp 0x7ffee6d10430 sp 0x7ffee6d10428
WRITE of size 4 at 0x60800000c578 thread T0
    #0 0x108f0b06a in SplashOutputDev::endType3Char(GfxState*) SplashOutputDev.cc:3079
    #1 0x108fb384c in Gfx::doShowText(GString*) Gfx.cc:3921
    #2 0x108f8a427 in Gfx::opShowSpaceText(Object*, int) Gfx.cc:3789
    #3 0x108f9f39d in Gfx::execOp(Object*, Object*, int) Gfx.cc:826
    #4 0x108f9e2fb in Gfx::go(int) Gfx.cc:719
    #5 0x108f9d185 in Gfx::display(Object*, int) Gfx.cc:641
    #6 0x1090a500e in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, int (*)(void*), void*) Page.cc:373
    #7 0x1090a49fe in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*), void*) Page.cc:321
    #8 0x1090b0902 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*)(void*), void*) PDFDoc.cc:432
    #9 0x108f1c721 in main pdftoppm.cc:229
    #10 0x7fff682412e4 in start (libdyld.dylib:x86_64+0x112e4)
```

ATTACHMENTS

pocfile.zip
(5.79 KiB) Downloaded 345 times

Mike Zhang of Pangu Lab

derekn

Re: heap-use-after-free in method SplashOutputDev::endType3Char

Tue Dec 03, 2019 8:55 pm

This was a bug introduced in a previous fix for nested Type 3 characters. That code wasn't correctly handling the case where a Type 3 char referred to another char in the same Type 3 font.

I'll have that fixed in the next release.

Thanks for the bug report.

mike

Re: heap-use-after-free in method SplashOutputDev::endType3Char

Fri Dec 06, 2019 3:15 am

Thanks for the description of the root cause!

Mike Zhang of Pangu Lab