Jump to bottom New issue

## SEGV (use after free) on Gfx::doShowText #35



⊙ Open ) strongcourage opened this issue on May 29, 2019 · 0 comments

```
strongcourage commented on May 29, 2019
Hi.
Our fuzzer found a crash due to an Use After Free bug on the function Gfx::doShowText (the latest commit b671b64 on master - version 0.70)
PoC: https://github.com/strongcourage/PoCs/blob/master/pdf2json b671b64/PoC uaf Gfx::doShowText
Valorind says:
     valgrind pdf2json $PoC /dev/null
==22556== Memcheck, a memory error detector
       ==22556== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
        ==22556== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
       ==22556== Command: ./pdf2json ./PoC_uaf_Gfx::doShowText /dev/null
     ...
=22556== Invalid read of size 8
=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=2256==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

=22556==

by @x46231: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64/pdf2json)

=22556==

=22556==

=22556==

by @x46827c: Gfx::doFoml(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64/pdf2json)

=22556==

=22556==

=22556==

=22556==

=22556==

Dy @x46827c: Gfx::doFoml(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64/pdf2json)

=22556==

=22556==

=2256==

=2256==

Dy @x46827c: Gfx::doFoml(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64/pdf2json)

=22556==

=22556==

=22556==

Dy @x46827c: Gfx::doFoml(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64/pdf2json)

=22556==

=2256==

=2256==

Dy @x46827c: Gfx::doFoml(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64/pdf2json)

=22556==

=2256==

=2256==

Dy @x46827c: Gfx::doFoml(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64/pdf2json)

=2256==

=2256==

=2256==

Dy @x46827c: Gfx::doFoml(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64/pdf2json)

=2256==

Dy @x46827c: Gfx::doFoml(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64/pdf2json)

=2256==

Dy @x46827c: Gfx::doFoml(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64/pdf2json)

=2256==

Dy @x46827c: Gfx::doFoml(Object*, int) (in /home/dungnguyen/PoCs/pdf2json) bg7lb64
      /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556== by 8x465CE0: Gfx::G6Fcm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 8x464230: Gfx::epxCbject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x45481D: Gfx::execOp(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x454531: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)

                                         at bx4CE7248: operator delete(void*) (in /usr/lib/valgrind/vgreload_memcheck-amd64-linux.so) by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
       ==22556==
        ==22556==
                                         by 0x45342: GfxResources::-GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4547C3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doFormI(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
       ==22556==
       ==22556==
==22556==
       /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                                        by 0x464328: 6fx::opX0bject(0bject*, int) (in /home/dungnguyen/PoCs/pdt2json_b671b64/pdf2json)
by 0x464318: 6fx::execOp(0bject*, 0bject*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454318: 6fx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: 6fx::display(0bject*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
       ==22556==
        ==22556==
       ==22556==
       ==22556== by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
       ==22556== Block was alloc'd at
==22556== at 0x4C2E0EF: opera
                                        JOCK WaS alloc d at d &AKCZEGE: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by &A659085: GFAFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PocS/pdf2json, b671b64/pdf2json) by &A659085: GFAFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json) by &A653388: GFAResources::GFAResources(XRef*, Dict*, GFAResources*) (in /home/dungngyyen/PocS/pdf2json_b671b64/pdf2json)
       ==22556==
       ==22556==
==22556==
       ==22556==
                                         by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
        ==22556==
       /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
       ==22556==
==22556==
                                         by 0.465C5E 64x::deFound(Deject*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0.4465C40 64x::deFound(Deject*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0.464230: Gfx::execOp(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0.454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
       ==22556==
                                         by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
       ==22556==
       ==22556==
        ==22556==
                                         by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
       /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
       ==22556== Invalid read of size 8
                                        valid read of size 8
at 0x40316F. HtmlString:HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:81)
by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
by 0x462C57: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46248E: Gfx::opShowText(Dbject*, int) (in /home/dungngy-/PoCs/pdf2json_b671b64/pdf2json)
by 0x4548BID: Gfx::execOp(Object*, Object*, int) (in /home/dungngy-opCoS/pdf2json_b671b64/pdf2json)
by 0x4548BID: Gfx::execOp(Object*, Object*, int) (in /home/dungngy-opCoS/pdf2json_b671b64/pdf2json)
        ==22556==
       ==22556==
       ==22556==
==22556==
       ==22556==
                                         by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, Function*, GfxColor*) (in
       ==22556==
       ==22556==
        ==22556==
      /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) ==22556== by 0x465CE0: Gfx::doForm(Object*) (
                                         by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                                         by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
       ==22556==
        ==22556==
                                  by 0x45436: 6fx::go(int) (in /home/dungguyen/PoCs/pdf2json)  
Address 0x552b0e0 is 160 bytes inside a block of size 4,584 free'd  
at 0x4C2F248: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
       ==22556==
       ==22556==
==22556==
                                         by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
       ==22556==
==22556==
                                         by 0x45342: GfxResources::-GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4547C3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doFormI(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
       ==22556==
        ==22556==
       ==22556==
       /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                                         by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
       ==22556==
        ==22556==
                                         by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_0671b64/pdf2json)
by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
       ==22556==
        ==22556==
       ==22556==
      ==22556== Block was alloc'd at
                                        at 0x4CZE0FF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
by 0x469005: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
```

```
==22556==
                               by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                               by Bx463612H: GTX:hontUlct::GTXFORIULCt(XARE'), NET, DACE () (AII JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/JAMME/
==22556==
==22556==
 ==22556==
                               by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) 
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                               by 0x464230: Gfx::opX0bject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                               by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454312: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==22556==
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556== Invalid read of size 8
                               ati 0x403238: HtmlString:HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:82) by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237) by 0x462C57: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
 ==22556==
                               by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
==22556==
==22556==
                               by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/POCS/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) 
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 0x464230: Gfx::oproblement of the control of the cont
                               at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json) by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
==22556==
==22556==
==22556==
==22556==
                               by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556== by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                              ==22556==
 ==22556==
==22556==
 ==22556==
==22556==
==22556==
                               by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
/home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==22556== Block was alloc'd at
==22556== at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                              at oxt.creer: operator new_unsigned long) (in /Usr/110/aygranu/oxgreadou_mem.retex-andou-airnux.so)
by 0x4690985: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46533800: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4650BB: Gfx::dosFormal(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
==22556==
  ==22556==
==22556==
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                              by 0x464230: Gfx::cubrom(Udject*) (in /indem/dungnguyen/Pocs/pdr2;pon)
by 0x464230: Gfx::cubrom(Udject*, int) (in /home/dungnguyen/Pocs/pdf2;pon)
by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/Pocs/pdf2;pon_b671b64/pdf2;pon)
by 0x454536: Gfx::go(int) (in /home/dungnguyen/Pocs/pdf2;pon_b671b64/pdf2;pon)
by 0x454513: Gfx::dsp(int) (in /home/dungnguyen/Pocs/pdf2;pon_b671b64/pdf2;pon)
by 0x454513: Gfx::dsp(int) (int) (in /home/dungnguyen/Pocs/pdf2;pon_b671b64/pdf2;pon)
by 0x42459E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) (in
==22556==
==22556==
==22556==
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
  ==22556== Invalid read of size 8
==22556==
                               at 0x40325C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:86)
                               at 0x40325C: htmlString::htmlString(GfxState*, double, double, MnlFontAccu*) (ImgOutputDev.cc:86)
by 0x4036Bit htmlPage::beginString(GfxState*, dotsTring*) (ImgOutputDev.cc:237)
by 0x462CS7: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x462A3E: Gfx::copShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B3D: Gfx::execOp(Object*, doublect*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B3S: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B3S: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B3S: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
==22556==
                               by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                               by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556== by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454536: Gfx::go(int) (in /home/dungnyen/PoCs/pdf2json_b671b64/pdf2json) address 0x5b2b058 is 24 bytes inside a block of size 4,584 free'd
                               at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
==22556==
==22556==
==22556==
                               by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                               by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                               by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
==22556==
  ==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                               by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
                               by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556==
                               by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== Block was alloc'd at
==22556==
                              at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                               by 0x469085: GfxFont::makeFont(XBef*, cha**, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x469086: GfxResources::GfxResources(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x453800: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
                               by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                               by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
==22556==
                               by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
                               by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==22556==
 ==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556== Invalid read of size 4
                              variur leau ur sizetength() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8v48C328: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8v48G328: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:88)
by 8v48G328C: HtmlString::HtmlString(GfxState*, double, double, MmlFontAccu*) (ImgOutputDev.cc:88)
==22556==
==22556==
==22556==
 ==22556==
==22556==
                               by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237) by 0x462C57: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                               by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
 ==22556==
                               by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
  ==22556==
                             by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, Function*, GfxColor*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by exactce: craft-acordinate period by the second period by the second period perio
                             by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
 ==22556==
                             by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 ==22556==
 ==22556==
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                             uyen;Pocs;Pours;Som_pos/10e4;Pours;Som)
by 0x465C50: 6fx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x464230: 6fx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: 6fx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
 ==22556==
  ==22556==
 ==22556==
                              by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556== Block was alloc'd at
                             at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload memcheck-amd64-linux.so)
 ==22556==
                             at exacterer: operator newtunisianed long) (in //usr/la/lov/augran/uygpreadd_mementer.-amobe-lanux.so)
by 0x468FTE: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in //home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
by 0x46FCFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in //home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
by 0x46FC63: GfxResources:(GfxResources(XRef*, Dict*, GfxResources*) (in //home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
by 0x46FC63: Gfx::pushResources(Dict*) (in //home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
 ==22556==
  ==22556==
 ==22556== by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                              by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
 ==22556==
                              by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
                            by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454511: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x45459E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) (in
 ==22556==
 ==22556==
 ==22556==
 ==22556==
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
  ==22556== Invalid read of size 8
                            valio read or Size o

at exade9088; GString::getCString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)

by 0x48C354: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)

by 0x486C354: XmlFont::XmlFont(GString*, int, double, GfxKGB) (XmlFonts.cc:88)

by 0x48326F: HtmlString;EfxString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==
  ==22556==
 ==22556==
 ==22556==
==22556==
 ==22556==
                              by 0x462C57: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                             by 0x4624816: Gfx::cgshowtex(Gbject*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454836: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
 ==22556==
                             by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 ==22556==
  ==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556== Address 0x5b2af58 is 8 bytes inside a block of size 16 free'd
                             at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x46947A: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
                             by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
                             by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                             by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 ==22556==
  ==22556==
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) 
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                             by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
 ==22556== Block was alloc'd at
==22556== at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                             As CAMLECER: Operator inextunising control in the control of the c
 ==22556==
 ==22556==
 ==22556==
  ==22556==
 ==22556== by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                             by 0x46SCE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
 ==22556==
                             by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
 ==22556==
                             by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
  ==22556== Invalid read of size 8
 ==22556==
                             at 0x4C326C8: memcpy@@GLIBC_2.14 (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                              by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
                             by 0x406434: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:88)
by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
 ==22556==
  ==22556==
 ==22556==
                             by 0x462C57: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json) by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
 ==22556==
==22556==
 ==22556==
                             by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                             by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 ==22556==
  ==22556==
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                              by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
 ==22556== Address 0x5b2afa0 is 0 bytes inside a block of size 16 free'd
 ==22556==
                             at 0x4C2F748: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                             by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
 ==22556==
                             by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                             by 0x4534F2: GfxResources::-GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doFormI(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, Function*, GfxColor*) (in
 ==22556==
 ==22556==
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                             by 0x464230: Gfx::opX0bject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556== Block was alloc'd at
  ==22556==
                              at 0x4C2E80F: operator new[](unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
 ==22556==
                             by 0x48E420: GString::resize(int) (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json) by 0x48C1C7: GString::GString(char const*) (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
  ==22556==
                             by 0x468F8C: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json
 ==22556==
  ==22556==
  ==22556==
                              by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
                         by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                         by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                         by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556==
                         by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556== Invalid read of size 2
                         at 0x4C32720: memcpy@GLIBC_2.14 (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                         toy exac.sou: ostring:isstring(string*) (in /nome/dungngyen/rocs/purijson_oo/zoo4/purijson) by 0x486434*, XmlFont::XmlFont(String*, int, double, 6rfxR6B) (XmlFonts.cc:88) by 0x40328C: HtmlString::HtmlString(6fxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88) by 0x40368C: HtmlPage::beginString(6fxState*, dString*) (ImgOutputDev.cc:30) by 0x402CS7: Gfx::doShowText(GString*) (in /home/dungngyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
 ==22556==
                         by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
                         by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json, b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, Function*, GfxColor*) (in
==22556==
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== Address 0x5b2afa8 is 8 bytes inside a block of size 16 free'd
==22556== at 0x4C2F748: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==
                         by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
                         by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                         by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                         by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x467C3: Gfx::pogResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466389: Gfx::doFormI(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, function*, GfxColor*) (in
==22556==
==22556==
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                         by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
==22556==
                          \  \, \text{by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json\_b671b64/pdf2json)} \\
 ==22556== Block was alloc'd at
                         at 0x4C2E80F: operator new[](unsigned long) (in /usr/lib/valgrind/vgpreload memcheck-amd64-linux.so)
==22556==
                         by 0x48E420: GString::resize(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x48E1C7: GString::GString(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                         by 0x468F8C: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungngyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x468FCB: GfxFontDict::GfxFontDict(XRef*, char*, Ref, Dict*) (in /home/dungngyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4538B0: GfxReSources:GfxReSources(XRef*, Dict*) (in /home/dungngyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4538B0: GfxReSources(XRef*, Dict*) (in /home/dungngyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungngyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
==22556==
==22556== by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                         by 0x465CEG 6fx::doFomO(Daject*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x465CEG 6fx::doFomO(Daject*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x464230: Gfx::execOp(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
                         by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
==22556== Invalid read of size 1
                         at 0x4C32758: memcpy@@GLIBC 2.14 (in /usr/lib/valgrind/vgpreload memcheck-amd64-linux.so)
==22556==
                         at oxxt.2273s: mem.pymmot.Int_Z.14 (In /us/110/valgrinu/wgpreioad_mem.nekk-amobe-linux.so) by 0x48(300) GString:GString(GString*) (in /home/dungnguyen/POCs/pdf2json_bStlb64/pdf2json) by 0x486434: XmlFont:XmlFont(GString*, int, double, GFXGB) (XmlFonts.cc:88) by 0x482362: HtmlString:HtmlString(GFXState*, double, double, MalFontAccu*) (ImgOutputDev.cc:88) by 0x48236B: HtmlPage::beginString(GfXState*, GString*) (ImgOutputDev.cc:237)
==22556==
==22556==
==22556==
 ==22556==
==22556==
                         by 0x462C57: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                         by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== Address 0x5b2afac is 12 bytes inside a block of size 16 free'd
                         at 0x4C2F74B: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556==
                         by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                         by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556==
                         by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
==22556==
==22556==
/home/dungn
                     nguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                         by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                         by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556== Block was alloc'd at
 ==22556==
                         at 0x4C2E80F: operator new[](unsigned long) (in /usr/lib/valgrind/vgpreload_m
                         As CARLECOR. Departure intelligents long (in /dsr/llD/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/valgrind/val
==22556==
 ==22556==
==22556==
==22556==
==22556==
==22556==
                         by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, Function*, GfxColor*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
                         by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                          by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                         by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556== Invalid read of size 4
                         at 0x41CA4E: GString::getLength() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x48C320: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x486C420: XmlFont::XmlFont(GString*, int, double, 6fxK6B) (XmlFontScc::88)
by 0x486A228C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==
==22556==
==22556==
 ==22556==
                         by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
by 0x462CS7: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556==
==22556==
==22556==
                         by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                         by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                         by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556== Address 0x5b2af50 is 0 bytes inside a block of size 16 free'd at 0x4C2F248: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                         by 0x46947A: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
 ==22556==
                         by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
                     by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==22556==
                     by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 ==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                     by 0x464230: Gfx::opX0bject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                     by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                  Block was alloc'd at
==22556==
                     at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                     at bxx_creer: operator new(unsigned long) (in /dsr/lid/yagrind/yagrindo/generotad_memcneck-amdow-linux.so)
by 0x468FE: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCS/pdf2json_b671b64/pdf2json)
by 0x4653380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46FCSB: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x465DBB: Gfx::doFormI(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, fint, Function*, GfxColor*) (in
==22556==
==22556==
==22556==
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                     by 0x465CE0: dfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x464230: dfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                     by 0x45481D: Gfx::excOptObject*, Jnt) (in /home/dungnguyen/PoCs/pdf2json_0671b64/pdf2json)
by 0x454831: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_0671b64/pdf2json)
by 0x454331: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_0671b64/pdf2json)
==22556==
 ==22556==
==22556==
==22556==
==22556== Invalid read of size 8
                     at 0x409098: GString::getCString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                     by 0x48C354: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                     by 0x4864441: XmlFont:XmlFont(Ostring*, int, double, 6fxK6B) (XmlFonts.cc:88)
by 0x486328C: HtmlString::HtmlString(6fxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
by 0x48328C: HtmlString::HtmlString(6fxState*, 6String*) (ImgOutputDev.cc:237)
by 0x48258C: 6fx::doShowText(Ostring*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
==22556==
==22556==
                     by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
                     by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 ==22556==
/home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==22556== by 8x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== Address 0x5b2af58 is 8 bytes inside a block of size 16 free'd
                    at 0x4CzF248: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x46547x: 0fxFont::-0fxFont() (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json) by 0x46CSD7: 0fxB0itFont::-0fxB0itFont() (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json) by 0x46CSD7: 0fx80itFont::-0fx80itFont() (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
==22556==
==22556==
==22556==
==22556==
                     by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556==
                     by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
==22556==
/home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
                     by 8x465CEG 6fx::doFomObject*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x465CEG 6fx::doFomObject* (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x464230: Gfx::execOp(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
                     by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556== Block was alloc'd at
==22556==
                     at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                     by 0x468F7E: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
                     by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                     by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, Function*, GfxColor*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                     by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                     by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
                     by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454312: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==22556==
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556== Invalid read of size 8
                     at 0x4C326C8: memcpy@@GLIBC_2.14 (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40644C: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:89)
==22556==
==22556==
==22556==
                     by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88) by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==
==22556==
                     by 0x4305B:: html/rage::negarstring(cfxxtate*, Gstring*) (ingoutputDev.Cc:2x)
by 0x462CS7: 6fx::doshowText(Gstring*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46243E: Gfx::coshowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454581D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454531: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454531: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
 ==22556==
==22556==
                     by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 ==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                     by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== Address 0x5b2afa0 is 0 bytes inside a block of size 16 free'd
                     at 0x4C2F74B: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
==22556==
==22556==
==22556==
                     by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                     by \ \texttt{0x46C5D7:} \ \texttt{Gfx8BitFont}:: \texttt{~Gfx8BitFont()} \ (\texttt{in /home/dungnguyen/PoCs/pdf2json\_b671b64/pdf2json)}
                     by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                     by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                      by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                     by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                     by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
==22556== Block was alloc'd at
                     at 0x4C2E80F: operator new[](unsigned long) (in /usr/lib/valgrind/vgpreload_m
                     by 0x48E420: GString::resize(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x48E420: GString::resize(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x48C1C7: GString::GString(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46SF8C: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46SF380: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x45S380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
==22556==
==22556==
                     by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                     by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                     by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                     by 0x464230: Gfx::opX0bject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                     by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556== Invalid read of size 2
```

```
==22556==
                            at 0x4C32720: memcpy@@GLIBC_2.14 (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                           by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x40644C: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:89)
by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
 ==22556==
 ==22556==
 ==22556==
                           by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237) by 0x462C57: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
   ==22556==
 ==22556==
                           by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                            by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
 ==22556==
 ==22556==
==22556==
                           by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/POCS/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== Address 0x5b2afa8 is 8 bytes inside a block of size 16 free'd
                           uuress 0x30z2ara6 is 8 0ytes inside a diotk of size in free d

at 0x4CE7746: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)

by 0x48C698: GString::-GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)

by 0x469472: GfxFont::-GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
 ==22556==
  ==22556==
 ==22556==
                           by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                            by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
==22556==
                           by 0x4534F2: GfxResources::-GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556== by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                           by 0x465CEB of fx::defom(Object*) (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
by 0x465CEB: 6fx::ofpxObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
by 0x464230: 6fx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b67lb64/pdf2json)
 ==22556==
 ==22556==
 ==22556==
   ==22556== Block was alloc'd at
                           Lock was alloc'd at at 0x4C2E86: operator new[](unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x48E420: GString::resize(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x48E420: GString::Gstring(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46E761: GString::Gstring(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46E761: GfxFontDict::GfxFontDict(XRef*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x45S380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
 ==22556==
 ==22556==
 ==22556==
 ==22556==
  ==22556==
 ==22556==
                            by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                           by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
 ==22556==
 ==22556==
==22556==
                           by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                            by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556== Invalid read of size 1
 ==22556==
                           at 0x4C32758: memcpy@@GLIBC_2.14 (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                           by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x40644C: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:89)
 ==22556==
==22556==
by 0x40644C: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:89)
by 0x406328C: HtmlString::HtmlString(GfxState*, double, double, MmlFontAccu*) (ImgOutputDev.cc:88)
by 0x406328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
by 0x40626F: Gfx::GstString*) (ImgOutputDev.cc:377)
by 0x462C57: Gfx::doShowText(GString*) (ImgOutputDev.cc:377)
by 0x462C57: Gfx::GstString*) (Int) (In
   ==22556==
 ==22556== by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== Address 0x5b2afac is 12 bytes inside a block of size 16 free'd
 ==22556==
                           at 0x4C2F74B: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so) by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==22556==
                           by 0x466472: GfxFont::~GfxBort() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466C587: Gfx8BitFont::~GfxBitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
 ==22556==
                           by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
 ==22556==
                           by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 ==22556==
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                           by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
 ==22556==
                           by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
 ==22556== Block was alloc'd at
  ==22556==
                           at 0x4C2E80F: operator new[](unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                           by 0x48E420: GString::resize(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                           by 0x48c1C1: GString::GString(:htm://lower/oungrugoyen/rocs/pdr2json/b071b04/pdr2json)
by 0x48C1C1: GString::GString(:htm://lower/oungrugoyen/rocs/pdr2json_b671b64/pdf2json)
by 0x46GER8: GfxFont::makeFont(KRef*, char*, Ref, Dict*) (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
by 0x46SER8: GfxFontDict::GfxFontDict(KRef*, Ref*, Dict*) (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
by 0x46SIR8: GfxResources::GfxResources(KRef*, Dict*, GfxResources*) (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
 ==22556==
 ==22556==
                           by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 ==22556==
   ==22556==
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                            by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==22556==
                           by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
  ==22556==
 ==22556==
 ==22556==
==22556== Invalid read of size 8
 ==22556==
                           at 0x4064E9: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:106) by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
                           by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
by 0x462C57: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
   ==22556==
 ==22556==
                            by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                             by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
                           by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, Function*, GfxColor*) (in
 ==22556==
 ==22556==
  ==22556==
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                            by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556== by 0x464230: Gfx::opX0bject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== Address 0x5b2af58 is 8 bytes inside a block of size 16 free'd
                           GOMESS MXSD23758 IS 8 Dytes Inslae a DIOCK or SIZE 16 TREE 0
at 8x4CE7248: operator delete(void*) (in /usr/li/valgrind/vgpreload_memcheck-amd64-linux.so)
by 8x465947A: 6fxFont::-6fxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x465587: 6fx8BitFont::-6fx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x465597: 6fx8BitFont:--6fx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
  ==22556==
 ==22556==
 ==22556==
==22556==
 ==22556==
                            by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                            by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                           by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
 ==22556==
   ==22556==
 /home/dungi
                          guyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
   ==22556==
                           by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
  ==22556==
                            by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
==22556== Block was alloc'd at
                        at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload memcheck-amd64-linux.so)
==22556==
                        at bXM_CLEBET: Option Table (unisplane) using (ini /usi/jia/ya/agi/alov/ggi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-inionia/agi/aload_memineck-ambov-in
==22556==
==22556==
                        by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556== by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in/home/dungnguyen/PoCs/pdf2json_0671b64/pdf2json)
                        by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json b671b64/pdf2json)
==22556==
                        by 0x464230: Gfx::opX0bject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                        by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454312: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
==22556==
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556== Invalid read of size 1
                       ard 0x577x570: _strcmp_sse2_unaligned (strcmp-sse2-unaligned.5:24)
by 0x406516: XmlFontc:XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:110)
by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
by 0x40368E: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
by 0x405257: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
==22556==
==22556==
                        by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x45481D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
                        by 0x4545316: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4545311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doFormI(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, Function*, GfxColor*) (in
==22556==
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556==
                        by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556==
                         by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
                        by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColor$pace*, int, int, int, Function*, GfxColor*) (in
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                        by 8x46SCEG 6fx::doFomObject*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x46SCEG 6fx::doFomObject*(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x46S4B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
==22556==
==22556== Block was alloc'd at
==22556== at 0x4C2E80F: operator new[](unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                        ==22556==
==22556==
==22556==
 ==22556==
==22556==
==22556==
                         by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                        by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                        by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556==
                         by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
==22556== Invalid read of size 4
                        at 0x467E4E: GfxFont::getType() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x462C66: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                        ==22556==
 ==22556==
==22556==
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                        by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                    oy 0x464298: Grx::opxUpject(upject*, int) (in /nome/dungnguyen/Poc/s/pdr2json_bo/1064/pdr2json) by 0x4548101: Gfx::exec(p(0)(bject*, object*, int) (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json) by 0x454536: Gfx::go(int) (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json) by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PocS/pdf2json_b671b64/pdf2json) Address 0x5b2b068 is 40 bytes inside a block of size 4.584 free'd at 0x4C2F248: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==
==22556==
==22556==
 ==22556==
 ==22556==
==22556==
                         by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                         by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                        by 0x45342: GfxResources::-GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4637C3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doFormI(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
==22556==
 ==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                        by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556==
                        by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b67b64/pdf2json)
==22556==
==22556==
==22556== by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556== Block was alloc'd at
                         at 0x4C2E0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
                        by 8x469905: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x46ECF8: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x453380: GfxReSources:GfxReSources(XRef*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
 ==22556==
==22556==
==22556==
                         by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, function*, GfxColor*) (in
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                        by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
                        by 0x464230: Gfx::opX0bject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                        by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454312: Page::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) (in
==22556==
==22556==
/home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) ==22556==
==22556== Invalid read of size 8
                       at 0x4636BD: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556==
 ==22556==
                        by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json, b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doFormI(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, Function*, GfxColor*) (in
==22556==
 ==22556==
==22556==
 /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
 ==22556==
                        by 0x465CE0: Gfx::doForm(Object*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
==22556==
                             by 0x464230: Gfx::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
                            by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json) by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556==
     ==22556==
     ==22556==
    by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556==
                            by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556==
                            by 0x467CC3: Gfx::popResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x466309: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
     ==22556==
     ==22556==
    ==22550== by 0x400309: GTX::U007UMI(U0]ect*, Ditt*, duole**, and, int, int, intx.OirSplet*, int, int, int, intx, i
     ==22556==
                            by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556==
                            ==22556==
     /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556== Block was alloc'd at
                           at 8x4CZE0EF: operator new(unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
by 8x469085: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x453886: GfxResources::GfxResources(XRef*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 8x453886: GfxResources(XRef*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556==
    ==22556==
     ==22556==
     ==22556==
                             by 0x465DBB: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
      ==22556==
    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyer/PoCs/pdf2json_b671b64/pdf2json)
by 0x42A59E: Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, Links*, int, Catalog*, int (*)(void*), void*) (in
     ==22556==
     /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556==
     pure virtual method called
     terminate called without an active exception
     ==22556==
     ==22556== Process terminating with default action of signal 6 (SIGABRT)
                            at 0x5710428: raise (raise.c:54)
by 0x5712029: abort (abort.c:89)
by 0x4EC984C: __gnu_cxx::__verbose_terminate_handler() (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21)
     ==22556==
     ==22556==
     ==22556==
                            by 0x4EC7685: ??? (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21) by 0x4EC7700: std::terminate() (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21)
     ==22556==
      ==22556==
     ==22556==
                            by 0x4EC823E: \_cxa\_pure\_virtual (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21) by 0x463726: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556==
                            by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556==
     ==22556==
     ==22556==
                            by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
     ==22556==
     /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
     ==22556==
    ==22556== HEAP SUMMARY:
     ==22556==
                               in use at exit: 321,643 bytes in 2,154 blocks
     ==22556==
                        total heap usage: 6,498 allocs, 4,344 frees, 577,716 bytes allocated
      ==22556==
     ==22556== LEAK SUMMARY:
                        definitely lost: 16 bytes in 1 blocks
     ==22556==
                           indirectly lost: 8 bytes in 1 blocks
                         possibly lost: 0 bytes in 0 blocks
still reachable: 321,619 bytes in 2,152 blocks
     ==22556==
     ==22556==
     ==22556==
                                                             of which reachable via heuristic:
     ==22556==
                                                                                                      : 264 bytes in 1 blocks
                                                                    newarray
     ==22556== suppressed: 0 bytes in 0 blocks
==22556== Rerun with --leak-check=full to see details of leaked memory
     ==22556==
     ==22556== For counts of detected and suppressed errors, rerun with: -v
     ==22556== ERROR SUMMARY: 33 errors from 18 contexts (suppressed: 0 from 0)
Thanks,
Manh Dung
```

Assignees

No one assigned

Labels

None yet

Projects None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

