New issue

Jump to bottom

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

Valgrind 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==
...
==22556== Invalid read of size 8
==22556==    at 0x462BD5: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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::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)
==22556==    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)
==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==  Address 0x5b2b040 is 0 bytes inside a block of size 4,584 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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)
==22556==    by 0x469005: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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 0x4031FB: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:81)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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::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)
==22556==    by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==  Address 0x5b2b0e0 is 160 bytes inside a block of size 4,584 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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)
==22556==    by 0x469005: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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 0x403238: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:82)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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::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)
==22556==    by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==  Address 0x5b2b0e8 is 168 bytes inside a block of size 4,584 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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)
==22556==    by 0x469005: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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 0x40325C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:86)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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::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)
==22556==    by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==  Address 0x5b2b058 is 24 bytes inside a block of size 4,584 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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)
==22556==    by 0x469005: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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 4
==22556==    at 0x41CA4E: GString::getLength() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x48C320: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x406434: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:88)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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 0x5b2af50 is 0 bytes inside a block of size 16 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46947A: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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)
==22556==    by 0x468F7E: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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
==22556==    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 0x406434: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:88)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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 0x5b2af58 is 8 bytes inside a block of size 16 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46947A: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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)
==22556==    by 0x468F7E: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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
==22556==    at 0x4C326C8: memcpy@@GLIBC_2.14 (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x406434: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:88)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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 0x5b2afa0 is 0 bytes inside a block of size 16 free'd
==22556==    at 0x4C2F74B: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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_b671b64/pdf2json)
==22556==    by 0x48C1C7: GString::GString(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x468F8C: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==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)
==22556==    by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x406434: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:88)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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
==22556==    at 0x4C2F74B: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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_b671b64/pdf2json)
==22556==    by 0x48C1C7: GString::GString(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x468F8C: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==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)
==22556==    by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x406434: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:88)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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 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)
==22556==    by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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_b671b64/pdf2json)
==22556==    by 0x48C1C7: GString::GString(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x468F8C: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556== Invalid read of size 4
==22556==    at 0x41CA4E: GString::getLength() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x48C320: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x40644C: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:89)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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 0x5b2af50 is 0 bytes inside a block of size 16 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46947A: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
```

```
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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)
==22556==    by 0x468F7E: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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 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 0x40644C: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:89)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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 0x5b2af58 is 8 bytes inside a block of size 16 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46947A: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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)
==22556==    by 0x468F7E: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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)
==22556==    by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x40644C: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:89)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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 0x5b2afa0 is 0 bytes inside a block of size 16 free'd
==22556==    at 0x4C2F74B: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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_b671b64/pdf2json)
==22556==    by 0x48C1C7: GString::GString(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x468F8C: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==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)
==22556==    by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x40644C: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:89)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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
==22556==    at 0x4C2F74B: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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_b671b64/pdf2json)
==22556==    by 0x48C1C7: GString::GString(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x468F8C: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==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)
==22556==    by 0x48C36D: GString::GString(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x40644C: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:89)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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 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)
==22556==    by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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_b671b64/pdf2json)
==22556==    by 0x48C1C7: GString::GString(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x468F8C: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556== Invalid read of size 8
==22556==    at 0x4064E9: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:106)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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::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)
==22556==  Address 0x5b2af58 is 8 bytes inside a block of size 16 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46947A: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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)
==22556==    by 0x468F7E: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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 1
==22556==    at 0x577A570: __strcmp_sse2_unaligned (strcmp-sse2-unaligned.S:24)
==22556==    by 0x406516: XmlFont::XmlFont(GString*, int, double, GfxRGB) (XmlFonts.cc:110)
==22556==    by 0x40328C: HtmlString::HtmlString(GfxState*, double, double, XmlFontAccu*) (ImgOutputDev.cc:88)
==22556==    by 0x4036BE: HtmlPage::beginString(GfxState*, GString*) (ImgOutputDev.cc:237)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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::opXObject(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==  Address 0x5b2afa0 is 0 bytes inside a block of size 16 free'd
==22556==    at 0x4C2F74B: operator delete[](void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x48C698: GString::~GString() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x469472: GfxFont::~GfxFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C587: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46C5D7: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    by 0x454B1D: Gfx::execOp(Object*, Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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_b671b64/pdf2json)
==22556==    by 0x48C1C7: GString::GString(char const*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x468F8C: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    by 0x454536: Gfx::go(int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==
==22556== Invalid read of size 4
==22556==    at 0x467E4E: GfxFont::getType() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x462C66: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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::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)
==22556==    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)
==22556==  Address 0x5b2b068 is 40 bytes inside a block of size 4,584 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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)
==22556==    by 0x469005: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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 0x4636BD: Gfx::doShowText(GString*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46243E: Gfx::opShowText(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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::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)
==22556==    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)
==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==  Address 0x5b2b040 is 0 bytes inside a block of size 4,584 free'd
==22556==    at 0x4C2F24B: operator delete(void*) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==22556==    by 0x46C5E3: Gfx8BitFont::~Gfx8BitFont() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46EEC9: GfxFontDict::~GfxFontDict() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x4534F2: GfxResources::~GfxResources() (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    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)
==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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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)
==22556==    by 0x469005: GfxFont::makeFont(XRef*, char*, Ref, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46ECFB: GfxFontDict::GfxFontDict(XRef*, Ref*, Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x453380: GfxResources::GfxResources(XRef*, Dict*, GfxResources*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x467C63: Gfx::pushResources(Dict*) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==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::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)
==22556==    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)
==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==
pure virtual method called
terminate called without an active exception
==22556==
==22556== Process terminating with default action of signal 6 (SIGABRT)
==22556==    at 0x5710428: raise (raise.c:54)
==22556==    by 0x5712029: abort (abort.c:89)
==22556==    by 0x4EC984C: __gnu_cxx::__verbose_terminate_handler() (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21)
==22556==    by 0x4EC76B5: ??? (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21)
==22556==    by 0x4EC7700: std::terminate() (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21)
==22556==    by 0x4EC823E: __cxa_pure_virtual (in /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21)
==22556==    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)
==22556==    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==    by 0x454311: Gfx::display(Object*, int) (in /home/dungnguyen/PoCs/pdf2json_b671b64/pdf2json)
==22556==    by 0x46627C: Gfx::doForm1(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*) (in
/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:
==22556==    definitely lost: 16 bytes in 1 blocks
==22556==    indirectly lost: 8 bytes in 1 blocks
==22556==      possibly lost: 0 bytes in 0 blocks
==22556==    still reachable: 321,619 bytes in 2,152 blocks
==22556==                       of which reachable via heuristic:
==22556==                         newarray           : 264 bytes in 1 blocks
==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)
Aborted
```

Thanks,
Manh Dung

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant