Closed Issue created 5 months ago by Mask6asok

Trigger a unhandled exception in GIMP 2.10.30

```
GNU Image Manipulation Program version 2.10.30
git-describe: Unknown, shouldn't happen
Build: org.gimp.GIMP_official rev 0 for windows
# C compiler #
        Using built-in specs.
        COLLECT_GCC=W:\msys64-gtk2\mingw64\bin\gcc.exe
        COLLECT_LTO_WRAPPER=W:/msys64-gtk2/mingw64/bin/../lib/gcc/x86_64-w64-mingw32/11.2.0/lto-wrap
        Target: x86_64-w64-mingw32
        Configured with: ../gcc-11.2.0/configure --prefix=/mingw64 --with-local-prefix=/mingw64/loca
        Thread model: posix
        Supported LTO compression algorithms: zlib zstd
        gcc version 11.2.0 (Rev5, Built by MSYS2 project)

# Libraries #
using babl version 0.1.88 (compiled against version 0.1.88)
using GEGL version 0.4.34 (compiled against version 0.4.34)
using GLib version 2.70.2 (compiled against version 2.70.2)
using GdkPixbuf version 2.42.6 (compiled against version 2.42.6)
using GTK+ version 2.24.33 (compiled against version 2.24.33)
using Pango version 1.50.2 (compiled against version 1.50.2)
using Fontconfig version 2.13.94 (compiled against version 2.13.94)
using Cairo version 1.17.4 (compiled against version 1.17.4)
```

fatal error: unhandled exception

Stack trace:

```
-------------------

Error occurred on Friday, June 3, 2022 at 15:37:43.

gimp-2.10.exe caused an Access Violation at location 00007FF692DE9E5C in module gimp-2.10.exe Writin

AddrPC           Params
00007FF692DE9E5C 000001C7F701D540 00007FF692DB3D5F 000001C700000000  gimp-2.10.exe!gimp_tool_cursors
00007FF692DB55A4 000001C7F5B001D0 0000007EBE1FEE90 000001C700000000  gimp-2.10.exe!gimp_tool_cursors
00007FF692DB6B74 0000007EBE1FEF52 00007FF6931F7610 0000000000000000  gimp-2.10.exe!gimp_tool_cursors
00007FF692C83BCF 000001C7EBD2D290 00007FFBB6D653A6 0000000000000000  gimp-2.10.exe!gimp_tool_cursors
00007FF692C7F340 000001C7EBDC8310 000001C7F663A430 000001C7B1B27370  gimp-2.10.exe!gimp_tool_cursors
00007FF692C7F4F9 000001C7EBDC8810 000001C7F4594560 0000000000000001  gimp-2.10.exe!gimp_tool_cursors
00007FF692D21BE0 000001C7EBEC7240 000001C7EBEF50B0 000001C700000003  gimp-2.10.exe!gimp_tool_cursors
00007FF692D14FF9 0000000000000003 00007FF692D14AF4 0000000000000000  gimp-2.10.exe!gimp_tool_cursors
00007FF692D0E43C 0000000000000000 0000000000000020 000001C7F7156780  gimp-2.10.exe!gimp_tool_cursors
00007FF692D0E8B7 000001C7EBE70C80 000001C7EBECA230 000001C7F663A430  gimp-2.10.exe!gimp_tool_cursors
00007FF692E304A4 0000000000000000 0000000000000000 000001C7F663A430  gimp-2.10.exe!gimp_core_pixbufs
00007FF692DDA679 000001C7EBD2D290 0000000000000000 0000000000000000  gimp-2.10.exe!gimp_tool_cursors
00007FF692DDA785 000001C7F7021760 000001C7F7043F10 000001C7F65BC168  gimp-2.10.exe!gimp_tool_cursors
00007FF692C4AE7C 000001C7B3B79860 00007FFBB6B5BB20 0000000000000000  gimp-2.10.exe!gimp_tool_cursors
00007FFBB6B58D47 000001C700000000 0000007EBE1FF688 000001C7B3B26870  libglib-2.0-0.dll!g_clear_list
00007FFBB6B5BEDE 0000000000000000 0000000000000000 000001C7EBD2D290  libglib-2.0-0.dll!g_main_contex
00007FFBB6B5C3FC 0000000000000000 0000000000000000 0000000000000000  libglib-2.0-0.dll!g_main_loop_r
00007FF692A31A2B 00007FFC2C7093B0 000001C7B1B4E480 000001C7B1C00860  gimp-2.10.exe!0x7ff600001a2b
00007FF692ECF67F 0000000000000000 000001C7B1B50E60 0000000000000000  gimp-2.10.exe!gimp_core_pixbufs
00007FF692A313B1 0000000000000000 0000000000000000 0000000000000000  gimp-2.10.exe!0x7ff6000013b1
00007FF692A314C6 0000000000000000 0000000000000000 0000000000000000  gimp-2.10.exe!0x7ff6000014c6
00007FFC2C7054E0 0000000000000000 0000000000000000 0000000000000000  KERNEL32.DLL!BaseThreadInitThun
00007FFC2E80485B 0000000000000000 0000000000000000 0000000000000000  ntdll.dll!RtlUserThreadStart

gimp-2.10.exe   2.10.30.0
ntdll.dll       10.0.22000.653
KERNEL32.DLL    10.0.22000.675
KERNELBASE.dll  10.0.22000.675
msvcrt.dll      7.0.22000.1
```

```
ole32.dll       10.0.22000.120
msvcp_win.dll   10.0.22000.1
ucrtbase.dll    10.0.22000.1
GDI32.dll       10.0.22000.1
win32u.dll      10.0.22000.675
gdi32full.dll   10.0.22000.675
USER32.dll      10.0.22000.282
combase.dll     10.0.22000.653
RPCRT4.dll      10.0.22000.675
SHELL32.dll     10.0.22000.593
libgimpmodule-2.0-0.dll
libgimpcolor-2.0-0.dll
libgimpmath-2.0-0.dll
libgimpconfig-2.0-0.dll
libgimpthumb-2.0-0.dll
libgimpwidgets-2.0-0.dll
libgimpbase-2.0-0.dll
exchndl.dll     0.8.2.0
PSAPI.DLL       10.0.22000.1
libbabl-0.1-0.dll
libcairo-2.dll
dbghelp.dll     6.3.9600.17298
libfontconfig-1.dll
libgdk_pixbuf-2.0-0.dll 2.42.6.0
libfreetype-6.dll       2.11.1.0
ADVAPI32.dll    10.0.22000.653
sechost.dll     10.0.22000.556
libgexiv2-2.dll
libgio-2.0-0.dll        2.70.2.0
libgobject-2.0-0.dll    2.70.2.0
libglib-2.0-0.dll       2.70.2.0
SHLWAPI.dll     10.0.22000.1
WS2_32.dll      10.0.22000.1
libharfbuzz-0.dll
libintl-8.dll   0.19.8.0
libjson-glib-1.0-0.dll
liblcms2-2.dll
libmypaint-0.dll
libpangoft2-1.0-0.dll   1.50.2.0
libpango-1.0-0.dll      1.50.2.0
libpangocairo-1.0-0.dll 1.50.2.0
zlib1.dll
libgdk-win32-2.0-0.dll  2.24.33.0
libgegl-0.4-0.dll
libgegl-npd-0.4.dll
libgtk-win32-2.0-0.dll  2.24.33.0
IMM32.dll       10.0.22000.1
libgmodule-2.0-0.dll    2.70.2.0
mscms.dll       10.0.22000.469
comdlg32.dll    10.0.22000.527
VERSION.dll     10.0.22000.1
shcore.dll      10.0.22000.613
MSIMG32.dll     10.0.22000.1
mgwhelp.dll     0.8.2.0
libgcc_s_seh-1.dll
libpixman-1-0.dll
libexpat-1.dll
libpng16-16.dll
libiconv-2.dll  1.16.0.0
gdiplus.dll     10.0.22000.675
libbz2-1.dll
libbrotlidec.dll
libstdc++-6.dll
libffi-7.dll
DNSAPI.dll      10.0.22000.653
IPHLPAPI.DLL    10.0.22000.282
USP10.dll       10.0.22000.1
libexiv2.dll
libwinpthread-1.dll     1.0.0.0
libpcre-1.dll
libgraphite2.dll
libjson-c-5.dll
```

libpangowin32-1.0-0.dll 1.50.2.0
libfribidi-0.dll
libthai-0.dll
COMCTL32.dll 5.82.22000.1
bcrypt.dll 10.0.22000.1
cfgmgr32.dll 10.0.22000.1
WINSPOOL.DRV 10.0.22000.675
libatk-1.0-0.dll 2.36.0.0
libbrotlicommon.dll
libcurl-4.dll
CRYPT32.dll 10.0.22000.348
WLDAP32.dll 10.0.22000.675
libdatrie-1.dll
libnghttp2-14.dll
libidn2-0.dll
libcrypto-1_1-x64.dll 1.1.1.12
libpsl-5.dll
libssh2-1.dll
libssl-1_1-x64.dll 1.1.1.12
libzstd.dll
libunistring-2.dll 0.9.10.0
NSI.dll 10.0.22000.1
windows.storage.dll 10.0.22000.675
wintypes.dll 10.0.22000.527
kernel.appcore.dll 10.0.22000.71
bcryptPrimitives.dll 10.0.22000.376
uxtheme.dll 10.0.22000.120
MSCTF.dll 10.0.22000.527
avx2-int8.dll
cairo.dll
CIE.dll
double.dll
fast-float.dll
float.dll
gegl-fixups.dll
gggl-lies.dll
gggl-table-lies.dll
gggl-table.dll
gggl.dll
gimp-8bit.dll
grey.dll
half.dll
HCY.dll
HSL.dll
HSV.dll
naive-CMYK.dll
simple.dll
sse-half.dll
sse2-float.dll
sse2-int16.dll
sse2-int8.dll
sse4-int8.dll
two-table.dll
u16.dll
u32.dll
ycbcr.dll
gegl-core.dll
profapi.dll 10.0.22000.1
OLEAUT32.dll 10.0.22000.1
clbcatq.dll 2001.12.10941.16384
propsys.dll 7.0.22000.37
apphelp.dll 10.0.22000.282
NetworkExplorer.dll 10.0.22000.51
winhttp.dll 10.0.22000.1
exr-load.dll
libIlmImf-2_5.dll
libIex-2_5.dll
libHalf-2_5.dll
libIlmThread-2_5.dll
libImath-2_5.dll
gegl-common-gpl3.dll
gegl-common.dll

```
gif-load.dll
jp2-load.dll
libjasper-4.dll
libjpeg-8.dll
jpg-load.dll
pdf-load.dll
libpoppler-glib-8.dll
libpoppler-115.dll
nss3.dll        3.73.1.0
libnspr4.dll    4.31.0.0
libplc4.dll     4.31.0.0
smime3.dll      3.73.1.0
libopenjp2-7.dll
libtiff-5.dll
libplds4.dll    4.31.0.0
nssutil3.dll    3.73.1.0
MSWSOCK.dll     10.0.22000.1
WINMM.dll       10.0.22000.1
libjbig-0.dll
libdeflate.dll
libLerc.dll
liblzma-5.dll   5.2.5.0
libwebp-7.dll
pixbuf-load.dll
png-load.dll
ppm-load.dll
raw-load.dll
libraw-20.dll
libgomp-1.dll
rgbe-load.dll
svg-load.dll
librsvg-2-2.dll
libcairo-gobject-2.dll
USERENV.dll     10.0.22000.1
libxml2-2.dll
text.dll
tiff-load.dll
webp-load.dll
exr-save.dll
jpg-save.dll
npy-save.dll
pixbuf-save.dll
png-save.dll
ppm-save.dll
rgbe-save.dll
sdl2-display.dll
SDL2.dll        2.0.18.0
SETUPAPI.dll    10.0.22000.469
tiff-save.dll
webp-save.dll
gegl-common-cxx.dll
lcms-from-profile.dll
npd.dll
path.dll
transformops.dll
vector-stroke.dll
seamless-clone-compose.dll
gegl-generated.dll
matting-levin.dll
libumfpack.dll
libamd.dll
libsuitesparseconfig.dll
libcholmod.dll
libcamd.dll
libccolamd.dll
libmetis.dll
libcolamd.dll
libopenblas.dll
libgfortran-5.dll
libquadmath-0.dll
seamless-clone.dll
libgegl-sc-0.4.dll
```

```
libwimp.dll
libpixmap.dll
libpixbufloader-png.dll
libpixbufloader-svg.dll
icm32.dll       10.0.22000.469
textinputframework.dll  10.0.22000.282
CoreMessaging.dll       10.0.22000.71
CoreUIComponents.dll    10.0.22000.132
CRYPTBASE.DLL   10.0.22000.1
PalmInputTSF.dll        2.7.0.1702
ntmarta.dll     10.0.22000.1
AppXDeploymentClient.dll        10.0.22000.469
urlmon.dll      11.0.22000.653
iertutil.dll    11.0.22000.653
netutils.dll    10.0.22000.434
srvcli.dll      10.0.22000.613
TextShaping.dll
Windows.ApplicationModel.dll    10.0.22000.593
mssprxy.dll     7.0.22000.593
mrmcorer.dll    10.0.22000.120
windows.staterepositorycore.dll 10.0.22000.65
windows.staterepositoryclient.dll       10.0.22000.653
bcp47mrm.dll    10.0.22000.65
Windows.UI.dll  10.0.22000.1
CRYPTSP.dll     10.0.22000.1
rsaenh.dll      10.0.22000.282
shfolder.dll    10.0.22000.1
webio.dll       10.0.22000.1
WINNSI.DLL      10.0.22000.1
SspiCli.dll     10.0.22000.556
rasadhlp.dll    10.0.22000.1
fwpuclnt.dll    10.0.22000.593
schannel.DLL    10.0.22000.675
mskeyprotect.dll        10.0.22000.1
NTASN1.dll      10.0.22000.1
ncrypt.dll      10.0.22000.1
ncryptsslp.dll  10.0.22000.1
MSASN1.dll      10.0.22000.1
DPAPI.DLL       10.0.22000.1
comctl32.dll    6.10.22000.120
WindowsCodecs.dll       10.0.22000.653

Windows 10.0.22000
DrMingw 0.8.2
```

Drag your designs here or click to upload.

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Activity

Jacob Boerema @Wormnest · 5 months ago — Developer

@Mask6asok Can you tell us what you were doing when this happened?

Mask6asok @Mask6asok · 5 months ago — Author

I made a XCF file and when i use gimp to open it, that happened

Please register or sign in to reply

Jacob Boerema added 1. Crash 2. Needs Information 2.10.30 OS: Windows labels 5 months ago

Mask6asok @Mask6asok · 5 months ago — Author

R12 is zero, so access to memory in 0x8c

Mask6asok @Mask6asok · 5 months ago — Author

crash.xcf This file can trigger it.

Jacob Boerema @Wormnest · 5 months ago — Developer

Thanks. I can reproduce and will work on improvements to our xcf loading code.

Did you create this using fuzzing. It doesn't look like a xcf that would be saved in the normal way.

If you are a security researcher and need to coordinate publication of details with us, then please let us know.

Mask6asok @Mask6asok · 5 months ago — Author

Yes, I am a security researcher, and I used AFL to find this crash on the previous version, so I tried it on the latest version and it still worked...

Jacob Boerema @Wormnest · 5 months ago — Developer

`gimp_channel_is_empty` returns FALSE if channel is NULL, see here. This causes `gimp_layer_invalidate_boundary` to crash here.

With a NULL channel `gimp_channel_is_empty` should return TRUE, just like the similar `gimp_image_is_empty` does.

Besides that, we should also more closely check image dimensions to be in a valid range, as well as offsets to layer and channel data.

Jehan @Jehan · 5 months ago — Maintainer

> Is that enough to apply for CVE?

@Mask6asok You are not forced to make a CVE. It's just that if you wish to make one, please tell us in advance. And if it's something possibly bad, ask the CVE maintainers to make it confidential at first (until release of the fix). If we need to make this report confidential too, we can.

But other than this, just reporting the issue, as you already did here (thanks for this!), and helping us fix it is already great, and creating a CVE is at your discretion. We don't care about existences or not of CVEs. We fix bugs because they are bugs and we want GIMP to evolve and be better, that's all.

The bottom line: CVE is unneeded but if you make one, communicate with us. Problems happen usually when bugs are irresponsibly spread on CVE databases (which have a lot of visibility) without communication.

> Can you tell me how to apply for a CVE ID.

We don't make CVE that often. I think this page details the process: https://oss-security.openwall.org/wiki/mailing-lists/oss-security (there is a CVE request link at the bottom)

But once again, you don't have to.

Please register or sign in to reply

Jacob Boerema changed milestone to %2.10.32 5 months ago

Jacob Boerema mentioned in commit 24c962b9 5 months ago

Jacob Boerema mentioned in commit a8428692 5 months ago

Jacob Boerema closed via commit 22af0bcf 5 months ago

Jacob Boerema mentioned in commit e7d4b580 5 months ago

Jacob Boerema mentioned in commit 74495943 5 months ago

Jacob Boerema mentioned in commit 6ab90ecb 5 months ago

Jacob Boerema @Wormnest · 5 months ago Developer

The crash is fixed in master and the 2.10 branch with

Edit (cited the wrong commit at first)

```
app: fix #8230 crash in gimp_layer_invalidate_boundary when channel is NULL

gimp_channel_is_empty returns FALSE if channel is NULL. This causes
gimp_layer_invalidate_boundary to crash if the mask channel is NULL.

With a NULL channel gimp_channel_is_empty should return TRUE, just like
the similar gimp_image_is_empty does, because returning FALSE here
suggests we have a non empty channel.
```

and

```
app: check max dimensions when loading xcf files

Improvements in loading broken xcf files, based on examining issue #8230.
Besides checking for a minimum width and height, GIMP also has a maximum
size we can and should check.

In the case of the image itself, we change invalid dimensions to a size of
1 in hope that the individual layers etc will have the correct size.
For layer, we will also try to go on, but for channel and layer mask, we
will give up.
```

The other two commits add some extra safety checks based on the other problems in the supplied XCF file.

We plan to release 2.10.32 "soon". We haven't discussed a new release for the development branch yet.

Edited by Jacob Boerema 5 months ago

Jacob Boerema mentioned in issue #1844 (closed) 5 months ago

Jacob Boerema mentioned in commit 22af0bcf 5 months ago

Mask6asok @Mask6asok · 4 months ago Author

CVE-2022-32990

Please register or sign in to reply