RSVG 2.40.13 / 2.42.2 - '.svg' Buffer Overflow

EDB-ID:
44491

CVE:
N/A

EDB Verified: ×

Author:
HAMM3R.PY

Type:
DOS

Exploit: / {}

Platform:
MULTIPLE

Date:
2018-04-18

Vulnerable App:

```
# Exploit Title: Buffer-overflow in RSVG while converting a malformed svg
# Date: 17 April 2018
# Exploit Author: Hamm3r.py
# Vendor Homepage: *https://launchpad.net/ubuntu/xenial/+package/librsvg2-
bin
# Software Link: *https://launchpad.net/ubuntu/xenial/+package/librsvg2-bin
# Version: Ubuntu: 2.40.13 (Default version that is shipped with ubuntu)
and MAC 2.42.2
# Tested on: Ubuntu 16.04 and MAC 10.13.3


RSVG throws a segmentation fault when malformed SVG is submitted as input.

Steps to reproduce:
rsvg test.png


GDB Stacktrace below:
Starting program: /usr/bin/rsvg fuzzed_fdiA0xdf5OQPYsN hello.png
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
_fill_xrgb32_lerp_opaque_spans (abstract_renderer=0x7fffffffbea0, y=18219,
h=1, spans=<optimized out>,
num_spans=<optimized out>) at
../../../../src/cairo-image-compositor.c:2249
2249 ../../../../src/cairo-image-compositor.c: No such file or directory.
(gdb) backtrace
#0 0x00007ffff6fd35c0 in _fill_xrgb32_lerp_opaque_spans
(abstract_renderer=0x7fffffffbea0, y=18219, h=1, spans=<optimized out>,
num_spans=<optimized out>) at ../../../../src/cairo-image-compositor.c:2249
#1 0x00007ffff7017921 in _cairo_tor_scan_converter_generate (xmax=248,
xmin=192, height=1, y=18219, spans=0x63e438, renderer=0x7fffffffbea0,
cells=<optimized out>)
at ../../../../src/cairo-tor-scan-converter.c:1643
#2 0x00007ffff7017921 in _cairo_tor_scan_converter_generate
(renderer=0x7fffffffbea0, antialias=1, winding_mask=<optimized out>,
converter=<optimized out>) at
../../../../src/cairo-tor-scan-converter.c:1794
#3 0x00007ffff7017921 in _cairo_tor_scan_converter_generate
(converter=0x63d3b0, renderer=0x7fffffffbea0)
at ../../../../src/cairo-tor-scan-converter.c:1857
#4 0x00007ffff7009c33 in composite_polygon
(extents=extents@entry=0x7fffffffd780,
polygon=polygon@entry=0x7fffffffd360,
fill_rule=fill_rule@entry=CAIRO_FILL_RULE_WINDING,
antialias=antialias@entry=CAIRO_ANTIALIAS_DEFAULT,
compositor=0x7ffff72b2040 <spans>, compositor=0x7ffff72b2040 <spans>)
at ../../../../src/cairo-spans-compositor.c:801
#5 0x00007ffff700a6a5 in clip_and_composite_polygon
(compositor=compositor@entry=0x7ffff72b2040 <spans>,
extents=extents@entry=0x7fffffffd780,
polygon=polygon@entry=0x7fffffffd360, fill_rule=CAIRO_FILL_RULE_WINDING,
antialias=antialias@entry=CAIRO_ANTIALIAS_DEFAULT) at
../../../../src/cairo-spans-compositor.c:967
#6 0x00007ffff700b5d3 in _cairo_spans_compositor_fill
(_compositor=0x7ffff72b2040 <spans>, extents=0x7fffffffd780,
path=<optimized out>, fill_rule=CAIRO_FILL_RULE_WINDING,
tolerance=0.10000000000000001, antialias=CAIRO_ANTIALIAS_DEFAULT) at
../../../../src/cairo-spans-compositor.c:1174
#7 0x00007ffff6fc5a90 in _cairo_compositor_fill (compositor=0x7ffff72b2040
<spans>, surface=0x6399a0, op=<optimized out>, source=<optimized out>,
path=0x639768, fill_rule=CAIRO_FILL_RULE_WINDING,
tolerance=0.10000000000000001, antialias=CAIRO_ANTIALIAS_DEFAULT, clip=0x0)
at ../../../../src/cairo-compositor.c:203
#8 0x00007ffff6fd7127 in _cairo_image_surface_fill
```

```
(abstract_surface=<optimized out>, op=<optimized out>, source=<optimized
out>, path=<optimized out>, fill_rule=<optimized out>, tolerance=<optimized
out>, antialias=<optimized out>, clip=0x0) at
../../../../src/cairo-image-surface.c:985
#9 0x00007ffff700e7d7 in _cairo_surface_fill (surface=0x6399a0,
op=CAIRO_OPERATOR_OVER, source=0x7fffffffdb50, path=0x639768,
fill_rule=CAIRO_FILL_RULE_WINDING, tolerance=0.10000000000000001,
antialias=CAIRO_ANTIALIAS_DEFAULT, clip=0x0) at
../../../../src/cairo-surface.c:2341
#10 0x00007ffff6fce14c in _cairo_gstate_fill (gstate=0x630c00,
path=path@entry=0x639768)
at ../../../../src/cairo-gstate.c:1317
#11 0x00007ffff6fc7279 in _cairo_default_context_fill
(abstract_cr=0x639400)
at ../../../../src/cairo-default-context.c:1055
#12 0x00007ffff6fc02b5 in cairo_fill (cr=0x639400) at
../../../../src/cairo.c:2205
#13 0x00007ffff7bc9e95 in () at /usr/lib/x86_64-linux-gnu/librsvg-2.so.2
#14 0x00007ffff7bc6272 in () at /usr/lib/x86_64-linux-gnu/librsvg-2.so.2
#15 0x00007ffff7bbd4c0 in () at /usr/lib/x86_64-linux-gnu/librsvg-2.so.2
#16 0x00007ffff7bbd4c0 in () at /usr/lib/x86_64-linux-gnu/librsvg-2.so.2
#17 0x00007ffff7bbd982 in () at /usr/lib/x86_64-linux-gnu/librsvg-2.so.2
#18 0x00007ffff7bbe298 in () at /usr/lib/x86_64-linux-gnu/librsvg-2.so.2
#19 0x00007ffff7bca9e3 in rsvg_handle_render_cairo_sub () at
/usr/lib/x86_64-linux-gnu/librsvg-2.so.2


Version:
$rsvg-convert --version
rsvg-convert version 2.42.2

#This issue is identified by Hamm3r.py, a general purpose fuzzer!


Proof of Concept:
https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-
sploits/44491.zip
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions