



Xfig Tickets

Xfig is a diagramming tool

Brought to you by: [tklxfiguser](#)

#65 stack-overflow in bezier_spline function



Milestone: [xfig](#)

Status: closed

Owner: nobody

Labels: None

Updated: 2020-12-21

Created: 2019-12-12

Creator: [Suhwan Song](#)

Private: No

Hi

I found a stack-overflow in bezier_spline function at genepic.c:1168

Please run following command to reproduce it,

```
fig2dev -L eepic $PoC
```

Here's log

.....

[illegible]

[illegible]

```
SUMMARY: AddressSanitizer: stack-overflow fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168 in bezi
==2423==ABORTING
```


I also tested this in git Commit [[3065ab](#)] and can reproduce it.

id:000231,sig:06,src:001219,op:havoc,rep:2


Tickets: ~~#127~~

tkl - 2020-01-26

- status: open --> pending




tkl - 2020-01-26




Fixed with commit [\[d70e4b\]](#).

Related

[Commit: \[d70e4b\]](#)




tkl - 2020-01-27




The fix with commit [\[d70e4b\]](#), to reject files containing '\0' anywhere, only hides the original issue. The cause for the stack overflow experienced here is that a spline with control points containing "inf" is read in and passed to bezier_spline.

Related


[Commit: \[d70e4b\]](#)




tkl - 2020-01-27




- status: pending --> open




tkl - 2020-01-29



- status: open --> pending




tkl - 2020-01-29




With commit [\[e3cee2\]](#), the range of the coordinates of the spline control points, which are floating point numbers, is now contained within the possible canvas of xfig figures, between INT_MIN and INT_MAX. Probably, one still might construct lethal splines.

Related

[Commit: \[e3cee2\]](#)



tkl - 2020-12-21



- status: pending --> closed
- xfig / fig2dev: fig2dev --> xfig

[Log in](#) to post a comment.

SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

Team

SourceForge Headquarters

225 Broadway Suite 1600

San Diego, CA 92101

+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status

