SEGV on unknown address 0x000000000000 (pc 0x55cc8b6086a6 bp 0x7ffed6538790 sp 0x7ffed6538740 T0) #183

Closed **p870613** opened this issue on Dec 22, 2021 · 1 comment · Fixed by #186

p870613 commented on Dec 22, 2021

Hi, I found a bug, SEGV.

- SUMMARY:
  SUMMARY: AddressSanitizer: SEGV (/home/lin/fribidi/bin/fribidi+0x66a5) in fribidi_remove_bidi_marks
- Version

```
➜  bin git:(master) ✗ ./fribidi --version
fribidi (GNU FriBidi) 1.0.11
interface version 4,
Unicode Character Database version 14.0.0,
Configure options.

Copyright (C) 2004  Sharif FarsiWeb, Inc.
Copyright (C) 2001, 2002, 2004, 2005  Behdad Esfahbod
Copyright (C) 1999, 2000, 2017, 2018, 2019  Dov Grobgeld
GNU FriBidi comes with NO WARRANTY, to the extent permitted by law.
You may redistribute copies of GNU FriBidi under
the terms of the GNU Lesser General Public License.
For more information about these matters, see the file named COPYING.

Written by Behdad Esfahbod and Dov Grobgeld
```

At branch `859aa1b`

- Steps to reproduce

```
git clone https://github.com/fribidi/fribidi.git
cd fribidi
./autogen.sh
```

```
CFLAGS=-fsanitize=address ./configure --disable-shared
make
./bin/fribidi --test  --novisual --basedir ./poc
```

- Platform

```
➜  bin git:(master) ✗ gcc --version
gcc (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0
Copyright (C) 2017 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

➜  bin git:(master) ✗  uname -r
5.4.0-91-generic
➜  bin git:(master) ✗ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.5 LTS
Release:        18.04
Codename:       bionic
```

- ASAN

```
➜  fribidi git:(master) ✗ ./bin/fribidi --test  --novisual --basedir
~/id:000194,sig:06,src:001474,op:arg1,rep:4
ASAN:DEADLYSIGNAL
=================================================================
==10834==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x55cc8b6086a6 bp
0x7ffed6538790 sp 0x7ffed6538740 T0)
==10834==The signal is caused by a READ memory access.
==10834==Hint: address points to the zero page.
    #0 0x55cc8b6086a5 in fribidi_remove_bidi_marks (/home/lin/fribidi/bin/fribidi+0x66a5)
    #1 0x55cc8b607d17 in main (/home/lin/fribidi/bin/fribidi+0x5d17)
    #2 0x7f41e828cbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #3 0x55cc8b606d29 in _start (/home/lin/fribidi/bin/fribidi+0x4d29)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/lin/fribidi/bin/fribidi+0x66a5) in
fribidi_remove_bidi_marks
==10834==ABORTING
```

poc: poc.zip

Thanks !!!

tagoh added a commit to tagoh/fribidi that referenced this issue on Feb 17

`Fix SEGV issue in fribidi_remove_bidi_marks` … e9167f3

tagoh mentioned this issue on Feb 17

Fix SEGV issue in fribidi_remove_bidi_marks #186

Merged

carnil commented on Mar 25

CVE-2022-25310 seems to have been assigned for this issue.

tagoh added a commit to tagoh/fribidi that referenced this issue on Mar 29

```
Fix SEGV issue in fribidi_remove_bidi_marks   …                                175850b
```

dov closed this as completed in #186 on Mar 30

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix SEGV issue in fribidi_remove_bidi_marks
tagoh/fribidi

2 participants