

[New issue](#)[Jump to bottom](#)

stack-buffer-overflow on address 0x7ffda2c0112f at pc 0x5580929d7ab5 bp 0x7ffda2bc1820 sp 0x7ffda2bc1810 #181

Closed

p870613 opened this issue on Dec 22, 2021 · 1 comment · Fixed by #184

p870613 commented on Dec 22, 2021 • edited

Hi, I found a bug, stack-buffer-overflow.

- SUMMARY:
AddressSanitizer: stack-buffer-overflow (/home/lin/fribidi/bin/fribidi+0x5ab4) in main
- Version

```
→ bin git:(master) X ./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 ./poc
```

- Platform

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

- ASAN

```
→ bin git:(master) X ./fribidi ~/id:000022,sig:06,src:000000,op:havoc,rep:128
=====
==8991==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffda2c0112f at pc
0x5580929d7ab5 bp 0x7ffda2bc1820 sp 0x7ffda2bc1810
READ of size 1 at 0x7ffda2c0112f thread T0
#0 0x5580929d7ab4 in main (/home/lin/fribidi/bin/fribidi+0x5ab4)
#1 0x7fb0cce3dbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
#2 0x5580929d6d29 in _start (/home/lin/fribidi/bin/fribidi+0x4d29)
```

```
Address 0x7ffda2c0112f is located in stack of thread T0 at offset 260191 in frame
#0 0x5580929d70d7 in main (/home/lin/fribidi/bin/fribidi+0x50d7)
```

```
This frame has 5 object(s):
```

```
[32, 36) 'option_index'
```

```
[96, 100) 'base'
```

```
[160, 260160) 'logical'
```

```
[260192, 325192) 'S_' <== Memory access at offset 260191 underflows this variable
```

```
[325248, 390248) 'outstring'
```

```
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or
swapcontext
```

```
(longjmp and C++ exceptions *are* supported)
```

```
SUMMARY: AddressSanitizer: stack-buffer-overflow (/home/lin/fribidi/bin/fribidi+0x5ab4) in main
```

```
Shadow bytes around the buggy address:
```

```
0x1000345781d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1000345781e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1000345781f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x100034578200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x100034578210: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x100034578220: 00 00 f2 f2 f2[f2]00 00 00 00 00 00 00 00 00 00
0x100034578230: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x100034578240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
0x100034578250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x100034578260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x100034578270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Shadow byte legend (one shadow byte represents 8 application bytes):

```
Addressable:          00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:      fa
Freed heap region:      fd
Stack left redzone:     f1
Stack mid redzone:      f2
Stack right redzone:    f3
Stack after return:     f5
Stack use after scope:  f8
Global redzone:         f9
Global init order:      f6
Poisoned by user:       f7
Container overflow:     fc
Array cookie:           ac
Intra object redzone:   bb
ASan internal:          fe
Left alloca redzone:    ca
Right alloca redzone:   cb
==8991==ABORTING
```

poc: [poc.zip](#)

Thanks !!!

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

 **Fix the stack buffer overflow issue** ...

ad3a19e

  **tagoh** mentioned this issue on Feb 17

Fix the stack buffer overflow issue #184

 **Merged**

 **dov** closed this as completed in [#184](#) on Feb 17

carnil commented on Mar 25

[CVE-2022-25308](#) seems to have been assigned to this issue.

No one assigned

Labels

None yet

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Fix the stack buffer overflow issue**
tagoh/fribidi

2 participants

