New issue

Jump to bottom

heap-buffer-overflow (/home/lin/fribidi/bin/fribidi+0x108fe) in fribidi_cap_rtl_to_unicode #182

Closed p870613 opened this issue on Dec 22, 2021 · 3 comments

p870613 commented on Dec 22, 2021

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

- SUMMARY:
  SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/lin/fribidi/bin/fribidi+0x108fe) in fribidi_cap_rtl_to_unicode

- 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 --caprtl ./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 --caprtl ~/id:000145,sig:06,src:000565,op:havoc,rep:4
����_f��������$
=================================================================
==10552==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61500000007c at pc
0x559f116818ff bp 0x7fffb37d3150 sp 0x7fffb37d3140
READ of size 4 at 0x61500000007c thread T0
    #0 0x559f116818fe in fribidi_cap_rtl_to_unicode (/home/lin/fribidi/bin/fribidi+0x108fe)
    #1 0x559f1168019e in fribidi_charset_to_unicode (/home/lin/fribidi/bin/fribidi+0xf19e)
    #2 0x559f11676b5e in main (/home/lin/fribidi/bin/fribidi+0x5b5e)
    #3 0x7f7d5fd4bbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #4 0x559f11675d29 in _start (/home/lin/fribidi/bin/fribidi+0x4d29)

0x61500000007c is located 4 bytes to the left of 512-byte region [0x615000000080,0x615000000280)
allocated by thread T0 here:
    #0 0x7f7d601f9b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x559f11680853 in init_cap_rtl (/home/lin/fribidi/bin/fribidi+0xf853)
    #2 0x559f116812b0 in fribidi_cap_rtl_to_unicode (/home/lin/fribidi/bin/fribidi+0x102b0)
    #3 0x559f1168019e in fribidi_charset_to_unicode (/home/lin/fribidi/bin/fribidi+0xf19e)
    #4 0x559f11676b5e in main (/home/lin/fribidi/bin/fribidi+0x5b5e)
    #5 0x7f7d5fd4bbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/lin/fribidi/bin/fribidi+0x108fe) in
fribidi_cap_rtl_to_unicode
Shadow bytes around the buggy address:
  0x0c2a7fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2a7fff8000: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]
  0x0c2a7fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0c2a7fff8020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff8030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
==10552==ABORTING
```

poc: poc.zip

Thanks !!!

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

`Fix the heap buffer overflow in fribidi_cap_rtl_to_unicode` ... `a1ccd5e`

tagoh mentioned this issue on Feb 17

Fix the heap buffer overflow in fribidi_cap_rtl_to_unicode #185

Closed

carnil commented on Mar 25

CVE-2022-25309 seems to have been assigned for this issue.

tagoh commented on Mar 29 Contributor

This seems to be fixed by `f22593b`

dov commented on Apr 19 Contributor

Yes, this has been fixed.

 **dov** closed this as completed on Apr 19

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix the heap buffer overflow in fribidi_cap_rtl_to_unicode
tagoh/fribidi

4 participants