

## DragonFlyBSD - Submit #2920

### `_ascii_wcsnrombs`, `_ascii_mbsnrto wcs`, and `_none_wcsnrombs` neglect to set `src` on EILSEQ error

06/08/2016 04:07 AM - RockinRoel

|  |               |                        |            |
|--|---------------|------------------------|------------|
| <b>Status:</b>   | Closed        | <b>Start date:</b>     | 06/08/2016 |
| <b>Priority:</b>   | Normal        | <b>Due date:</b>       |            |
| <b>Assignee:</b>   | dragonflybsd1 | <b>% Done:</b>         | 0%         |
| <b>Category:</b>   |               | <b>Estimated time:</b> | 0.00 hour  |
| <b>Target version:</b>   |               |                        |            |
| <b>Description</b>   |               |                        |            |
| DragonFlyBSD's libc also suffers from this bug in FreeBSD and Mac OS X:<br><a href="https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=209907">https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=209907</a>   |               |                        |            |
| I noticed that when using <code>wcsrtombs</code> , if a character is encountered that can not be converted, it sets <code>errno</code> to <code>EILSEQ</code> and returns <code>(size_t)-1</code> . However <code>*src</code> still points to the original character, even though it should point to the character after the one that conversion stopped at. I've attached a test program that reproduces the issue. |               |                        |            |
| The expected output is:<br>inptr - in: 7   |               |                        |            |
| The actual output is:<br>inptr - in: 0   |               |                        |            |
| I've included the patch that fixes it for the none and ascii locale (it's fine for other locales).   |               |                        |            |

## History

### #1 - 06/09/2016 03:02 AM - yellowrabbit2010

- File `eilseq_fix_corrected_2.patch` added
- Tracker changed from Bug to Submit

corrected patch from RockinRoel and, while we are here fix possible NULL pointer dereference.

### #2 - 06/09/2016 03:11 AM - dragonflybsd1

- Assignee set to `dragonflybsd1`

### #3 - 06/19/2016 02:11 AM - dragonflybsd1

Committed: <https://gitweb.dragonflybsd.org/dragonfly.git/commitdiff/9915e371b196ef063ed0bfddd33e797cd03c61ea>

Thanks guys!

### #4 - 06/18/2019 09:39 AM - liweitianux

The patch has been committed in 2016.

### #5 - 06/18/2019 09:39 AM - liweitianux

- Status changed from New to Closed

## Files

| File Name                                 | Size       | Date       | Author           |
|---|------------|------------|------------------|
| <code>test_wcsrtombs.c</code>             | 312 Bytes  | 06/08/2016 | RockinRoel       |
| <code>eilseq_fix.patch</code>             | 1006 Bytes | 06/08/2016 | RockinRoel       |
| <code>eilseq_fix_corrected_2.patch</code> | 1.32 KB    | 06/09/2016 | yellowrabbit2010 |