

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

Use Box<T> instead of Vec<T> to initialize and drop ArrayQueue #533

[Merged](#) 1 commit merged into [crossbeam-rs:master](#) from [caelunshun:no-vec-with-capacity](#) on Aug 4, 2020

Conversation 9 Commits 1 Checks 0 Files changed 3

**caelunshun** commented on Jun 26, 2020 • edited[Contributor](#)

Previously, the queue buffer was initialized using `Vec::from_iter` through `collect`. Note that `collect` does not guarantee a precise capacity; the layout of the allocated memory could have a greater size.

`ArrayVec::drop` assumed the buffer has a size equal to the queue's capacity. This is undefined behavior when the buffer actually has a different size thanks to `vec`.

Using `Box<T>` instead guarantees an exact capacity, resolving the UB.

(The same fix should probably be applied to [concurrent-queue](#) as it suffers from the same bug.)

[Use Box<T> instead of Vec<T> to initialize and drop ArrayQueue](#) ...

be327d5

[caelunshun](#) force-pushed the `no-vec-with-capacity` branch from [769c195](#) to [be327d5](#) 2 years ago[Compare](#)**Gilnaa** commented on Jul 2, 2020

The `FromIterator` [impl](#) that `collect` uses for `Box<T>` is

```
impl<A> FromIterator<A> for Box<A> {
    fn from_iter<T: IntoIterator<Item = A>>(iter: T) -> Self {
        iter.into_iter().collect::<Vec<A>>().into_boxed_slice()
    }
}
```

I might be wrong, but wouldn't this also result in bigger than needed allocation?

caelunshun commented on Jul 2, 2020 • edited[Contributor](#) [Author](#)

The `FromIterator` [impl](#) that `collect` uses for `Box<T>` is

```
impl<A> FromIterator<A> for Box<A> {
    fn from_iter<T: IntoIterator<Item = A>>(iter: T) -> Self {
        iter.into_iter().collect::<Vec<A>>().into_boxed_slice()
    }
}
```

I might be wrong, but wouldn't this also result in bigger than needed allocation?

`into_boxed_slice` [will shrink the allocation's size to the length of the slice](#):

```
unsafe {
    self.shrink_to_fit();
    let me = ManuallyDrop::new(self);
    let buf = ptr::read(&me.buf);
    let len = me.len();
    buf.into_box(len).assume_init()
}
```

Notice the call to `shrink_to_fit`.

[caelunshun](#) mentioned this pull request on Aug 3, 2020**Memory Leak in crossbeam-queue ArrayQueue? (Latest git only, ver0.2.3 is not effected) #539**[Closed](#)**ghost** approved these changes on Aug 4, 2020[View changes](#)**ghost** left a comment

Thank you!

ghost merged commit [772b4f3](#) into [crossbeam-rs:master](#) on Aug 4, 2020[sticnarf](#) mentioned this pull request on Aug 24, 2020**crossbeam-channel 0.4 has undefined behavior** [tikv/tikv#8492](#)

🔒 Closed

🔗  **taiki-e** mentioned this pull request on Aug 25, 2020

refactor: re-export crossbeam-channel nervosnetwork/ckb#2244

🔗 Merged

🔗 **bors**  added a commit to nervosnetwork/ckb that referenced this pull request on Sep 1, 2020

 Merge #2244 ...

✓ 2832363

taiki-e commented on Sep 30, 2020

Member

@**rocallehan** crossbeam-channel 0.4.4 is like removing [the commit that introduced the UB fixed by this PR](#) from 0.4.3. So "incorrect layout on deallocation" UB shouldn't exist in that version. (Could you check the output of `cargo tree | grep 'crossbeam-channel' ?`)

rocallehan commented on Sep 30, 2020


Yes, I just figured that out and deleted my comment, sorry.

I was confused because I couldn't find the commit from this PR under the crossbeam-channel-0.4.4 tag. I also looked at the 0.4.4 crates.io source and misunderstood the code there. Thanks!

rocallehan commented on Oct 1, 2020 • edited


I do think it would be good if fixes for critical bugs like this can make it into a release more quickly. It was more than two months from this bug being discovered and the fix submitted (late June) to 0.4.4 being released and 0.4.3 being yanked (early September). We updated to 0.4.3 in the meantime and I guess a lot of other projects did too.

🔗 **moz-v2v-gh** pushed a commit to mozilla/gecko-dev that referenced this pull request on Oct 7, 2020

 Bug 1668514 - Update crossbeam-channel. r=janerik ...

c314a37

🔗 **moz-v2v-gh** pushed a commit to mozilla/gecko-dev that referenced this pull request on Oct 7, 2020

 Bug 1668514 - Update crossbeam-channel. r=janerik, a=jcristau ...

9586429

tomrittervg commented on Oct 8, 2020

Would it be possible to request a CVE from Github for this issue?

🔗  **taiki-e** mentioned this pull request on Oct 11, 2020


Add advisory for UB in crossbeam-channel 0.4.3 rustsec/advisory-db#425

🔗 Merged

taiki-e commented on Oct 11, 2020

Member

@**tomrittervg** I've filed advisory in [rustsec/advisory-db#425](#). (And I'll request a CVE from Github.)

🔗  **ktff** mentioned this pull request on Oct 11, 2020

Resolve RUSTSEC-2020-0052 vectordotdev/vector#4515

🔒 Closed

🔗 **sidvishnoi** pushed a commit to sidvishnoi/gecko-webmonetization that referenced this pull request on Oct 13, 2020

 Bug 1668514 - Update crossbeam-channel. r=janerik ...

74632ce

taiki-e commented on Oct 14, 2020 • edited

Member

Security advisory is now published as [RUSTSEC-2020-0052](#) / [GHSA-v5m7-53cv-f3hx](#) / [CVE-2020-15254](#).

🔗  **jdm** mentioned this pull request on Nov 21, 2020

Update past yanked crate. servo/servo#27788

🔗 Merged

📋 3 tasks

🔗 **bors-servo** added a commit to servo/servo that referenced this pull request on Nov 21, 2020


 Auto merge of #27788 - jdm:crossbeam-channel-up, r=jdm ...

✗ deee433

🔗 **bors-servo** added a commit to servo/servo that referenced this pull request on Nov 22, 2020

 Auto merge of #27788 - jdm:crossbeam-channel-up, r=jdm ...

✗ 66616c6

🔗  **taiki-e** mentioned this pull request on Jan 21

Reduce unsafe code in array queue/bounded channel #774

➔ Merged

bors (bot) added a commit that referenced this pull request on Jan 22

Merge #774

✓ 6465d5e

CJS77 added a commit to tari-project/broadcast_channel that referenced this pull request on Jun 7

bug: update crossbeam-channel

✗ 659ca76

CJS77 mentioned this pull request on Jun 7

bug: update crossbeam-channel tari-project/broadcast_channel#4

➔ Merged

CJS77 added a commit to tari-project/broadcast_channel that referenced this pull request on Jun 7

bug: update crossbeam-channel

✗ 60f9e2c

CJS77 added a commit to tari-project/broadcast_channel that referenced this pull request on Jun 7

bug: update crossbeam-channel

✓ eaa8b1a

CJS77 added a commit to tari-project/broadcast_channel that referenced this pull request on Jun 7

bug: update crossbeam-channel (#4)

✓ 8aa6dd2

This pull request was closed.

Reviewers

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

5 participants

