

New issue

Jump to bottom

# String::retain allows safely creating invalid (non-utf8) strings when abusing panic #78498

**Closed** SkiFire13 opened this issue on Oct 28, 2020 · 1 comment · Fixed by #78499

Labels C-bug I-unsound P-high T-libs T-libs-api

SkiFire13 commented on Oct 28, 2020 Contributor

While `String::retain` executes it may temporarily leave the `String` in an inconsistent state, in particular it may contain invalid utf8. This is safe because it restores this invariant before returning, but the caller may skip this by panicing inside the closure and catching the unwind it outside. This allows to create `String` `s` that are not utf8, breaking the library invariant without using `unsafe`.

For example the following will panic at the final assertion, while I would expect it to never fail when `s` has type `String`:

```
let mut s = "000".to_string();
let _ = std::panic::catch_unwind(std::panic::AssertUnwindSafe(|| {
    let mut count = 0;
    s.retain(|_| {
        count += 1;
        match count {
            1 => false,
            2 => true,
            _ => panic!(),
        }
    });
}));
assert!(std::str::from_utf8(s.as_bytes()).is_ok()); // This will fail
```

SkiFire13 added the C-bug label on Oct 28, 2020

SkiFire13 mentioned this issue on Oct 28, 2020

Prevent `String::retain` from creating non-utf8 strings when abusing panic #78499

**Merged**

jonas-schievink added I-unsound T-libs labels on Oct 28, 2020

rustbot added the I-prioritize label on Oct 28, 2020

camelid added P-high and removed I-prioritize labels on Oct 28, 2020

camelid commented on Oct 28, 2020 Member

Assigning P-high and removing I-prioritize as discussed in the prioritization working group.

camelid added the T-libs-api label on Oct 28, 2020

SkiFire13 added a commit to SkiFire13/rust that referenced this issue on Oct 29, 2020

Added test for issue rust-lang#78498 3860e50

jonas-schievink pushed a commit to jonas-schievink/rust that referenced this issue on Oct 29, 2020

Added test for issue rust-lang#78498 1f6f917

bors closed this as completed in 48c4afb on Oct 29, 2020

Qwaz mentioned this issue on Dec 21, 2020

Update `unsound DrainFilter` and `RString::retain` rodrimati1992/abi\_stable\_crates#44

**Closed**


rodrimati1992 added a commit to rodrimati1992/abi\_stable\_crates that referenced this issue on Dec 21, 2020

Fixed `String::retain`, `RVec::retain`. Bumped patch version to 0.9.1 . ... bfdbd14

Qwaz mentioned this issue on Dec 21, 2020



Add advisories for standard library soundness bugs rustsec/advisory-db#539

**Closed**

 **rodrimati1992** added a commit to rodrimati1992/abi\_stable\_crates that referenced this issue on Dec 21, 2020

 0 9.1 patch (#45) ...

✓ 342de83

  **Qwaz** mentioned this issue on Jan 13, 2021

**Add advisory for rust-lang/rust#78498** rustsec/advisory-db#561

 Closed

  **ammaraskar** mentioned this issue on Feb 19, 2021

**Update unsound SmallString::Retain** murarth/smallstr#12

 Closed

 **rodrimati1992** added a commit to rodrimati1992/abi\_stable\_crates that referenced this issue last month

 0 9.1 patch (#45) ...

5b941e0

Assignees

No one assigned

Labels

**C-bug** I-unsound **P-high** T-libs T-libs-api

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Prevent String::retain from creating non-utf8 strings when abusing panic**  
SkiFire13/rust

4 participants

