<> Code   ⊙ Issues 87   ⋃ Pull requests 27   ⊙ Actions   ⛊ Security 3   ⮑ Insights

Unsoundness of AtomicCell<{i,u}64> arithmetics on 32-bit targets that support Atomic{I,U}64

(High) **taiki-e** published **GHSA-qc84-gqf4-9926** on Feb 14

Package

Ⓡ **crossbeam-utils** (Rust)

Affected versions

<= 0.8.6

Patched versions

>= 0.8.7

Description

Impact

The affected version of this crate incorrectly assumed that the alignment of `{i,u}64` was always the same as `Atomic{I,U}64`.

However, the alignment of `{i,u}64` on a 32-bit target can be smaller than `Atomic{I,U}64`.

This can cause the following problems:

- Unaligned memory accesses
- Data race

Crates using `fetch_*` methods with `AtomicCell<{i,u}64>` are affected by this issue.

32-bit targets without `Atomic{I,U}64` and 64-bit targets are not affected by this issue.
32-bit targets with `Atomic{I,U}64` and `{i,u}64` have the same alignment are also not affected by this issue.

The following is a complete list of the builtin targets that may be affected. (last update: nightly-2022-02-11)

- armv7-apple-ios (tier 3)
- armv7s-apple-ios (tier 3)

- i386-apple-ios (tier 3)
- i586-unknown-linux-gnu
- i586-unknown-linux-musl
- i686-apple-darwin (tier 3)
- i686-linux-android
- i686-unknown-freebsd
- i686-unknown-haiku (tier 3)
- i686-unknown-linux-gnu
- i686-unknown-linux-musl
- i686-unknown-netbsd (tier 3)
- i686-unknown-openbsd (tier 3)
- i686-wrs-vxworks (tier 3)

([script to get list](#))

Patches

This has been fixed in crossbeam-utils 0.8.7.

Affected 0.8.x releases have been yanked.

References

[#781](#)

License

This advisory is in the public domain.

Severity

High

CVE ID

CVE-2022-23639

Weaknesses

No CWEs