RUSTSEC-2020-0046

bespoke Cell implementation allows obtaining several mutable references to the same data

Reported	January 8, 2020
Issued	October 2, 2020 (last modified: October 19, 2021)
Package	actix-service (crates.io)
Type	INFO Unsound
Categories	memory-corruption
Aliases	CVE-2020-35899
Details	https://github.com/actix/actix-net/pull/158
CVSS Score	5.5 MEDIUM
CVSS Details	

Attack vector	Local
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
Patched	`>=1.0.6`

Description

The custom implementation of a Cell primitive in the affected versions of this crate does not keep track of mutable references to the underlying data.

This allows obtaining several mutable references to the same object which may result in arbitrary memory corruption, most likely use-after-free.

The flaw was corrected by switching from a bespoke `Cell<T>` implementation to `Rc<RefCell<T>>`.