



Look up package or ID...

[About](#) [Advisories](#) [Report Vulnerabilities](#)



RUSTSEC-2020-0131

[History](#) · [Edit](#)

Send/Sync bound needed on T for Send/Sync impl of RcuCell

Reported November 14, 2020

Issued January 30, 2021 (last modified: October 19, 2021)

Package [rcu_cell](#) ([crates.io](#))

Type Vulnerability

Categories [memory-corruption](#)
[thread-safety](#)

Aliases [CVE-2020-36451](#)

Details https://github.com/Xudong-Huang/rcu_cell/issues/3

CVSS Score 8.1 HIGH

CVSS Details

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

CVSS Vector [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

Patched no patched versions

Description

Affected versions of this crate unconditionally implement Send/Sync for `RcuCell<T>`. This allows users to send `T: !Send` to other threads (while `T` enclosed within `RcuCell<T>`), and allows users to concurrently access `T: !Sync` by using the APIs of `RcuCell<T>` that provide access to `&T`.

This can result in memory corruption caused by data races.