RUSTSEC-2020-0142

History · Edit

Send bound needed on T (for Send impl of `Bucket2`)

Reported	November 29, 2020
Issued	February 2, 2021 (last modified: October 19, 2021)
Package	syncpool (crates.io)
Type	Vulnerability
Categories	memory-corruption
Aliases	CVE-2020-36462
Details	https://github.com/Chopinsky/byte_buffer/issues/2
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	`>=0.1.6`

Description

Affected versions of this crate unconditionally implements `Send` for `Bucket2`. This allows sending non-Send types to other threads.

This can lead to data races when non Send types like `Cell<T>` or `Rc<T>` are contained inside `Bucket2` and sent across thread boundaries. The data races can potentially lead to memory corruption (as demonstrated in the PoC from the original report issue).

The flaw was corrected in commit 15b2828 by adding a `T: Send` bound to the `Send` impl of `Bucket2<T>`.