RUSTSEC-2020-0135

History · Edit

Slock allows sending non-Send types across thread boundaries

Reported	November 17, 2020	
Issued	January 30, 2021 (last modified: November 27, 2022)	
Package	slock (crates.io)	
Type	Vulnerability	
Categories	memory-corruption thread-safety	
Aliases	CVE-2020-36455	
Details	https://github.com/BrokenLamp/slock-rs/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	`>=0.2.0`	

Description

`Slock<T>` unconditionally implements `Send` / `Sync`.

Affected versions of this crate allows sending non-Send types to other threads, which can lead to data races and memory corruption due to the data race.