RUSTSEC-2020-0151

History · Edit

Generators can cause data races if non-Send types are used in their generator functions

Reported	November 16, 2020	
Issued	March 30, 2021 (last modified: October 19, 2021)	
Package	generator (crates.io)	
Type	Vulnerability	
Categories	memory-corruption	
Keywords	#concurrency	
Aliases	CVE-2020-36471	
Details	https://github.com/Xudong-Huang/generator-rs/issues/27	
CVSS Score	5.9 MEDIUM	
CVSS Details	Attack vector	Network
	Attack complexity	High
	Privileges required	None
	User interaction	None
	Scope	Unchanged
	Confidentiality	None
	Integrity	None
	Availability	High
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	
Patched	`>=0.7.0`	

Description

The `Generator` type is an iterable which uses a generator function that yields values. In affected versions of the crate, the provided function yielding values had no `Send` bounds despite the `Generator` itself implementing `Send`.

The generator function lacking a `Send` bound means that types that are dangerous to send across threads such as `Rc` could be sent as part of a generator, potentially leading to data races.

This flaw was fixed in commit `f7d120a3b` by enforcing that the generator function be bound by `Send`.