RUSTSEC-2020-0108

Soundness issue: Input can be misused to create data race to an object

Reported	December 20, 2020
Issued	January 20, 2021 (last modified: October 19, 2021)
Package	eventio (crates.io)
Type	Vulnerability
Categories	memory-corruption
	thread-safety
Aliases	CVE-2020-36216
Details	https://github.com/petabi/eventio/issues/33
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	`>=0.5.1`

Description

`Input<R>` implements `Send` without requiring `R: Send`.

Affected versions of this crate allows users to send non-Send types to other threads, which can lead to undefined behavior such as data race and memory corruption.

The flaw was corrected in version 0.5.1 by adding `R: Send` bound to the `Send` impl of `Input<R>`.