



Look up package or ID...

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



RUSTSEC-2020-0143

[History](#) · [Edit](#)

Queues allow non-Send types to be sent to other threads, allowing data races

Reported	December 25, 2020																
Issued	February 4, 2021 (last modified: October 19, 2021)																
Package	multiqueue (crates.io)																
Type	Vulnerability																
Categories	memory-corruption thread-safety																
Aliases	CVE-2020-36463																
Details	https://github.com/schets/multiqueue/issues/31																
CVSS Score	8.1 HIGH																
CVSS Details	<table><tr><td>Attack vector</td><td>Network</td></tr><tr><td>Attack complexity</td><td>High</td></tr><tr><td>Privileges required</td><td>None</td></tr><tr><td>User interaction</td><td>None</td></tr><tr><td>Scope</td><td>Unchanged</td></tr><tr><td>Confidentiality</td><td>High</td></tr><tr><td>Integrity</td><td>High</td></tr><tr><td>Availability</td><td>High</td></tr></table>	Attack vector	Network	Attack complexity	High	Privileges required	None	User interaction	None	Scope	Unchanged	Confidentiality	High	Integrity	High	Availability	High
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 implemented `Send` for types used in queue implementations (`InnerSend<RW, T>` , `InnerRecv<RW, T>` , `FutInnerSend<RW, T>` , `FutInnerRecv<RW, T>`).

This allows users to send non-Send types to other threads, which can lead to data race bugs or other undefined behavior.