RUSTSEC-2021-0047

SliceDeque::drain_filter can double drop an element if the predicate panics

Reported	February 19, 2021
Issued	March 30, 2021 (last modified: October 19, 2021)
Package	slice-deque (crates.io)
Type	Vulnerability
Categories	memory-corruption
Keywords	#memory-safety #double-free
Aliases	CVE-2021-29938
Details	https://github.com/gnzlbg/slice_deque/issues/90
CVSS Score	7.5 HIGH

CVSS Details

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Patched	no patched versions

Description

Affected versions of the crate incremented the current index of the drain filter iterator *before* calling the predicate function `self.pred`.

If the predicate function panics, it is possible for the last element in the iterator to be dropped twice.