RUSTSEC-2021-0018

History · Edit

insert_slice_clone can double drop if Clone panics.

Reported	February 3, 2021
Issued	February 4, 2021 (last modified: October 19, 2021)
Package	qwutils (crates.io)
Type	Vulnerability
Categories	memory-corruption
Keywords	#memory-safety #double-free
Aliases	CVE-2021-26954
Details	https://github.com/qwertz19281/rust_utils/issues/3
CVSS Score	5.3 MEDIUM
CVSS Details	

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

CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
Patched	>=0.3.1

Affected Functions	Version
`qwutils::imp::vec::VecExt::insert_slice_clone`	<0.3.1

Description

Affected versions of this crate used `ptr::copy` when inserting into the middle of a `Vec`. When ownership was temporarily duplicated during this copy, it calls the clone method of a user provided element.

This issue can result in an element being double-freed if the clone call panics.

Commit `20cb73d` fixed this issue by adding a `set_len(0)` call before operating on the vector to avoid dropping the elements during a panic.