RUSTSEC-2021-0010

History · Edit

panic safety: double drop may happen within `util::{mutate, mutate2}`

Reported	January 12, 2021	
Issued	January 20, 2021 (last modified: October 19, 2021)	
Package	containers (crates.io)	
Type	Vulnerability	
Categories	memory-corruption	
Aliases	CVE-2021-25907	
Details	https://github.com/strake/containers.rs/issues/2	
CVSS Score	9.8 CRITICAL	
CVSS Details		
	Attack vector	Network
	Attack complexity	Low
	Privileges required	None
	User interaction	None
	Scope	Unchanged
	Confidentiality	High
	Integrity	High
	Availability	High
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
Patched	`>=0.9.11`	

Description

Upon panic in a user-provided function `f`, `fn mutate()` & `fn mutate2` drops twice a same object.

Affected versions of this crate did not guard against double drop while temporarily duplicating an object's ownership with `ptr::read()`.

Dropping a same object can result in memory corruption.

The flaw was corrected in version "0.9.11" by fixing the code to abort upon panic.