RUSTSEC-2021-0049

History · Edit

`through` and `through_and` causes a double free if the map function panics

Reported	February 18, 2021
Issued	March 30, 2021 (last modified: October 19, 2021)
Package	through (crates.io)
Type	Vulnerability
Categories	memory-corruption
Keywords	#memory-safety #double-free
Aliases	CVE-2021-29940
Details	https://github.com/gretchenfrage/through/issues/1
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	no patched versions

Description

`through` and `through_and` take a mutable reference as well as a mapping function to change the provided reference. They do this by calling `ptr::read` on the reference which duplicates ownership and then calling the mapping function.

If the mapping function panics, both the original object and the one duplicated by `ptr::read` get dropped, causing a double free.