RUSTSEC-2020-0149

History · Edit

Data race and memory safety issue in `Index`

Reported	November 15, 2020
Issued	March 30, 2021 (last modified: October 19, 2021)
Package	appendix (crates.io)
Type	Vulnerability
Categories	memory-corruption thread-safety
Aliases	CVE-2020-36469
Details	https://github.com/krl/appendix/issues/6
CVSS Score	5.9 MEDIUM
CVSS Details	

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

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

Description

The `appendix` crate implements a key-value mapping data structure called `Index<K, V>` that is stored on disk. The crate allows for any type to inhabit the generic `K` and `V` type parameters and implements Send and Sync for them unconditionally.

Using a type that is not marked as `Send` or `Sync` with `Index` can allow it to be used across multiple threads leading to data races. Additionally using reference types for the keys or values will lead to the segmentation faults in the crate's code.