RUSTSEC-2020-0023

History · Edit

Lifetime boundary for `raw_slice` and `raw_slice_mut` are incorrect

Reported	February 11, 2020
Issued	October 2, 2020 (last modified: October 19, 2021)
Package	rulinalg (crates.io)
Type	Vulnerability
Aliases	CVE-2020-35879
Details	https://github.com/AtheMathmo/rulinalg/issues/201
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
Unaffected	`<0.4.0`

Affected Functions	Version
`rulinalg::matrix::RowMut::raw_slice`	`>=0.4.0`
`rulinalg::matrix::RowMut::raw_slice_mut`	`>=0.4.0`

Description

The affected version of `rulinalg` has incorrect lifetime boundary definitions for `RowMut::raw_slice` and `RowMut::raw_slice_mut`. They do not conform with Rust's borrowing rule and allows the user to create multiple mutable references to the same location. This may result in unexpected calculation result and data race if both references are used at the same time.