History · Edit

RUSTSEC-2020-0152

ImmediateIO and TransactionalIO can cause data races

Reported	December 18, 2020
Issued	March 30, 2021 (last modified: October 19, 2021)
Package	max7301 (crates.io)
Type	Vulnerability
Categories	memory-corruption
Keywords	#concurrency
Aliases	CVE-2020-36472
Details	https://github.com/edarc/max7301/issues/1
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	`>=0.2.0`

Description

The `ImmediateIO` and `TransactionalIO` types implement `Sync` for all contained `Expander<EI>` types regardless of if the `Expander` itself is safe to use across threads.

As the `IO` types allow retrieving the `Expander`, this can lead to non-thread safe types being sent across threads as part of the `Expander` leading to data races.