History · Edit

RUSTSEC-2021-0072

Task dropped in wrong thread when aborting `LocalSet` task

Reported	July 7, 2021
Issued	July 7, 2021 (last modified: November 6, 2021)
Package	tokio (crates.io)
Type	Vulnerability
Categories	memory-corruption
Keywords	#race-condition #send
Aliases	CVE-2021-38191
Details	https://github.com/tokio-rs/tokio/issues/3929
Patched	`>=1.5.1, <1.6.0`
	`>=1.6.3, <1.7.0`
	`>=1.7.2, <1.8.0`
	`>=1.8.1`
Unaffected	`<0.3.0`

Affected Functions	Version
`tokio::task::JoinHandle::abort`	`<=1.8.0, >=0.3.0`

Description

When aborting a task with `JoinHandle::abort`, the future is dropped in the thread calling abort if the task is not currently being executed. This is incorrect for tasks spawned on a `LocalSet`.

This can easily result in race conditions as many projects use `Rc` or `RefCell` in their Tokio tasks for better performance.

See tokio#3929 for more details.