RUSTSEC-2020-0052

History · Edit

Undefined Behavior in bounded channel

Reported	June 26, 2020
Issued	October 11, 2020 (last modified: January 4, 2021)
Package	crossbeam-channel (crates.io)
Type	Vulnerability
Categories	memory-corruption
Aliases	CVE-2020-35904 CVE-2020-15254 GHSA-v5m7-53cv-f3hx
Details	https://github.com/crossbeam-rs/crossbeam/pull/533
Patched	`>=0.4.4`
Unaffected	`<0.4.3`

Description

The affected version of this crate's the `bounded` channel incorrectly assumes that `Vec::from_iter` has allocated capacity that same as the number of iterator elements. `Vec::from_iter` does not actually guarantee that and may allocate extra memory. The destructor of the `bounded` channel reconstructs `Vec` from the raw pointer based on the incorrect assumes described above. This is unsound and causing deallocation with the incorrect capacity when `Vec::from_iter` has allocated different sizes with the number of iterator elements.