RUSTSEC-2020-0130

History · Edit

Bunch unconditionally implements Send/Sync

Reported	November 12, 2020
Issued	January 30, 2021 (last modified: October 19, 2021)
Package	bunch (crates.io)
Type	Vulnerability
Categories	memory-corruption thread-safety
Aliases	CVE-2020-36450
Details	https://github.com/krl/bunch/issues/1
CVSS Score	8.1 HIGH
CVSS Details	

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

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

Description

Affected versions of this crate unconditionally implements `Send` / `Sync` for `Bunch<T>`. This allows users to insert `T: !Sync` to `Bunch<T>`. It is possible to create a data race to a `T: !Sync` by invoking the `Bunch::get()` API (which returns `&T`) from multiple threads. It is also possible to send `T: !Send` to other threads by inserting `T` inside `Bunch<T>` and sending `Bunch<T>` to another thread, allowing to create a data race by inserting types like `T = Rc<_>`.

Such data races can lead to memory corruption.