RUSTSEC-2020-0097

Soundness issue with base::Error

Reported	December 10, 2020
Issued	January 18, 2021 (last modified: October 19, 2021)
Package	xcb (crates.io)
Type	INFO Unsound
Categories	memory-corruption
	thread-safety
Aliases	CVE-2020-36205
Details	https://github.com/rtbo/rust-xcb/issues/93
CVSS Score	5.5 MEDIUM

CVSS Details

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

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

Description

`base::Error` type contains public field named `ptr`. With this definition, it is possible to create a `base::Error` with an invalid pointer and trigger memory safety errors such as use-after-free or double-free with safe Rust.

The users of `xcb` crate are advised not to manipulate the field.