



Look up package or ID...

[About](#) [Advisories](#) [Report Vulnerabilities](#)



RUSTSEC-2020-0005

[History](#) · [Edit](#)

CBox API allows to de-reference raw pointers without `unsafe` code

Reported March 19, 2020

Issued October 2, 2020 (last modified: October 19, 2021)

Package [cbox](#) ([crates.io](#))

Type Vulnerability

Categories [memory-corruption](#)

Aliases [CVE-2020-35860](#)

Details <https://github.com/TomBebbington/cbox-rs/issues/2>

CVSS Score 9.8 CRITICAL

CVSS Details

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

CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

Patched no patched versions

Description

`CBox` and `CSemiBox` are part of the public API of the `cbox` crate and they allow to create smart pointers from raw pointers and de-reference them without the need of `unsafe` code.