RUSTSEC-2020-0079

History · Edit

`socket2` invalidly assumes the memory layout of std::net::SocketAddr

Reported	November 6, 2020
Issued	December 2, 2020 (last modified: October 19, 2021)
Package	socket2 (crates.io)
Type	INFO Unsound
Keywords	#memory #layout #cast
Aliases	CVE-2020-35920
Details	https://github.com/rust-lang/socket2-rs/issues/119
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	`>=0.3.16`

Description

The `socket2` crate has assumed `std::net::SocketAddrV4` and `std::net::SocketAddrV6` have the same memory layout as the system C representation `sockaddr`. It has simply casted the pointers to convert the socket addresses to the system representation. The standard library does not say anything about the memory layout, and this will cause invalid memory access if the standard library changes the implementation. No warnings or errors will be emitted once the change happens.