



Look up package or ID...

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



RUSTSEC-2021-0021

[History](#) · [Edit](#)

`nb-connect` invalidly assumes the memory layout of `std::net::SocketAddr`

Reported February 14, 2021

Issued February 14, 2021 (last modified: October 19, 2021)

Package [nb-connect](#) ([crates.io](#))

Type INFO Unsound

Keywords [#memory](#) [#layout](#) [#cast](#)

Aliases [CVE-2021-27376](#)

Details <https://github.com/smol-rs/nb-connect/issues/1>

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 [>=1.0.3](#)

Description

The `nb-connect` 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.