RUSTSEC-2020-0049

History · Edit

Use-after-free in Framed due to lack of pinning

Reported	January 30, 2020
Issued	October 2, 2020 (last modified: October 19, 2021)
Package	actix-codec (crates.io)
Type	Vulnerability
Categories	memory-corruption
Aliases	CVE-2020-35902
Details	https://github.com/actix/actix-net/issues/91
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	`>=0.3.0-beta.1`

Description

Affected versions of this crate did not require the buffer wrapped in `Framed` to be pinned, but treated it as if it had a fixed location in memory. This may result in a use-after-free.

The flaw was corrected by making the affected functions accept `Pin<&mut Self>` instead of `&mut self`.