RUSTSEC-2020-0048

History · Edit

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

Reported	January 24, 2020	
Issued	October 2, 2020 (last modified: October 19, 2021)	
Package	actix-http (crates.io)	
Type	Vulnerability	
Categories	memory-corruption	
Aliases	CVE-2020-35901	
Details	https://github.com/actix/actix-web/issues/1321	
CVSS Score	7.5 HIGH	
CVSS Details		
	Attack vector	Network
	Attack complexity	Low
	Privileges required	None
	User interaction	None
	Scope	Unchanged
	Confidentiality	None
	Integrity	None
	Availability	High
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	
Patched	`>=2.0.0-alpha.1`	

Description

Affected versions of this crate did not require the buffer wrapped in `BodyStream` 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 trait `MessageBody` require `Unpin` and making `poll_next()` function accept `Pin<&mut Self>` instead of `&mut self`.