RUSTSEC-2021-0007

History · Edit

`Frame::copy_from_raw_parts` can lead to segfault without `unsafe`

Reported	January 7, 2021
Issued	January 19, 2021 (last modified: October 19, 2021)
Package	av-data (crates.io)
Type	Vulnerability
Categories	memory-exposure privilege-escalation
Aliases	CVE-2021-25904
Details	https://github.com/rust-av/rust-av/issues/136
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	`>=0.3.0`

Description

`fn Frame::copy_from_raw_parts()` is a safe API that can take a raw pointer and dereference it. It is possible to read arbitrary memory address with an arbitrarily fed pointer. This allows the safe API to access & read arbitrary address in memory. Feeding an invalid memory address pointer to the API may also cause the program to segfault.

The flaw was corrected in https://github.com/rust-av/rust-av/pull/137, by removing the API `fn Frame::copy_from_raw_parts()` .