RUSTSEC-2021-0014

History · Edit

Record::read : Custom `Read` on uninitialized buffer may cause UB

Reported	January 26, 2021
Issued	January 27, 2021 (last modified: October 19, 2021)
Package	marc (crates.io)
Type	Vulnerability
Categories	memory-exposure
Aliases	CVE-2021-26308
Details	https://github.com/blackbeam/rust-marc/issues/7
CVSS Score	7.5 HIGH
CVSS Details	

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	None
Availability	None

CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Patched	`>=2.0.0`

Description

Affected versions of this crate passes an uninitialized buffer to a user-provided `Read` implementation. (`Record::read()`)

Arbitrary `Read` implementations can read from the uninitialized buffer (memory exposure) and also can return incorrect number of bytes written to the buffer. Reading from uninitialized memory produces undefined values that can quickly invoke undefined behavior.

This flaw was fixed in commit 6299af0 by zero-initializing the newly allocated memory (via `data.resize(len, 0)`) instead of exposing uninitialized memory (`unsafe { data.set_len(len) }`).