RUSTSEC-2021-0015

History · Edit

`Sectors::get` accesses unclaimed/uninitialized memory

Reported	January 6, 2021
Issued	January 30, 2021 (last modified: October 19, 2021)
Package	calamine (crates.io)
Type	Vulnerability
Categories	memory-corruption
	memory-exposure
Aliases	CVE-2021-26951
Details	https://github.com/tafia/calamine/issues/199
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	`>=0.17.0`

Description

Affected versions of this crate arbitrarily calls `Vec::set_len` to increase length of a vector without claiming more memory for the vector. Affected versions of this crate also calls user-provided `Read` on the uninitialized memory of the vector that was extended with `Vec::set_len`.

This can overwrite active entities in adjacent heap memory and seems to be a major security issue. Also, calling user-provided `Read` on uninitialized memory is defined as UB in Rust.