RUSTSEC-2020-0007

History · Edit

use-after or double free of allocated memory

Reported	March 27, 2020
Issued	October 2, 2020 (last modified: October 19, 2021)
Package	bitvec (crates.io)
Type	Vulnerability
Categories	memory-corruption
Aliases	CVE-2020-35862
Details	https://github.com/myrrlyn/bitvec/issues/55
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	`>=0.17.4`
Unaffected	`<0.11.0`

Affected Functions	Version
`bitvec::vec::BitVec::into_boxed_bitslice`	`<0.17.4, >=0.11.0`

Description

Conversion of `BitVec` to `BitBox` did not account for allocation movement.

The flaw was corrected by using the address after resizing, rather than the original base address.