History · Edit

RUSTSEC-2020-0146

arr! macro erases lifetimes

Reported	April 9, 2020
Issued	March 1, 2021 (last modified: October 19, 2021)
Package	generic-array (crates.io)
Type	Vulnerability
Categories	memory-corruption
Keywords	#soundness
Aliases	CVE-2020-36465
Details	https://github.com/fizyk20/generic-array/issues/98
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	`>=0.8.4, <0.9.0`
`>=0.9.1, <0.10.0`
`>=0.10.1, <0.11.0`
`>=0.11.2, <0.12.0`
`>=0.12.4, <0.13.0`
`>=0.13.3`
Unaffected	`<0.8.0`

Description

Affected versions of this crate allowed unsoundly extending lifetimes using `arr!` macro. This may result in a variety of memory corruption scenarios, most likely use-after-free.