RUSTSEC-2020-0047

History · Edit

array_queue pop_back() may cause a use-after-free

Reported	September 26, 2020	
Issued	October 2, 2020 (last modified: October 19, 2021)	
Package	array-queue (crates.io)	
Type	Vulnerability	
Keywords	#memory-corruption #uninitialized-memory #use-after-free	
Aliases	CVE-2020-35900	
Details	https://github.com/raviqqe/array-queue/issues/2	
CVSS Score	5.5 MEDIUM	
CVSS Details	Attack vector	Local
	Attack complexity	Low
	Privileges required	Low
	User interaction	None
	Scope	Unchanged
	Confidentiality	High
	Integrity	None
	Availability	None
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	
Patched	no patched versions	
Unaffected	`<0.3.0`	

Description

array_queue implements a circular queue that wraps around an array. However, it fails to properly index into the array in the `pop_back` function allowing the reading of previously dropped or uninitialized memory.