RUSTSEC-2020-0145

Use-after-free when cloning a partially consumed `Vec` iterator

Reported	November 2, 2020
Issued	February 27, 2021 (last modified: October 19, 2021)
Package	heapless (crates.io)
Type	INFO Unsound
Categories	memory-corruption memory-exposure
Keywords	#use-after-free
Aliases	CVE-2020-36464
Details	https://github.com/japaric/heapless/issues/181
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	`>=0.6.1`

Affected Functions	Version
`heapless::vec::IntoIter::clone`	`<=0.6`

Description

The `IntoIter` `Clone` implementation clones the whole underlying `Vec`. If the iterator is partially consumed the consumed items will be copied, thus creating a use-after-free access.

A proof of concept is available in the original bug report.