RUSTSEC-2021-0048

StackVec::extend can write out of bounds when size_hint is incorrect

Reported	February 19, 2021
Issued	March 30, 2021 (last modified: October 19, 2021)
Package	stackvector (crates.io)
Type	Vulnerability
Categories	memory-corruption
Aliases	CVE-2021-29939
Details	https://github.com/Alexhuszagh/rust-stackvector/issues/2
CVSS Score	7.3 HIGH
CVSS Details	

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	Low

CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
Patched	`>=1.0.9`

Description

`StackVec::extend` used the lower and upper bounds from an Iterator's `size_hint` to determine how many items to push into the stack based vector.

If the `size_hint` implementation returned a lower bound that was larger than the upper bound, `StackVec` would write out of bounds and overwrite memory on the stack. As mentioned by the size_hint documentation, `size_hint` is mainly for optimization and incorrect implementations should not lead to memory safety issues.