RUSTSEC-2021-0003

Buffer overflow in SmallVec::insert_many

Reported	January 8, 2021
Issued	January 8, 2021 (last modified: October 19, 2021)
Package	smallvec (crates.io)
Type	Vulnerability
Categories	memory-corruption
Keywords	#buffer-overflow #heap-overflow #unsound
Aliases	CVE-2021-25900
Details	https://github.com/servo/rust-smallvec/issues/252
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	`>=0.6.14, <1.0.0` `>=1.6.1`
Unaffected	`<0.6.3`

Affected Functions	Version
`smallvec::SmallVec::insert_many`	`>=0.6.3, <0.6.14` `>=1.0.0, <1.6.1`

Description

A bug in the `SmallVec::insert_many` method caused it to allocate a buffer that was smaller than needed. It then wrote past the end of the buffer, causing a buffer overflow and memory corruption on the heap.

This bug was only triggered if the iterator passed to `insert_many` yielded more items than the lower bound returned from its `size_hint` method.

The flaw was corrected in smallvec 0.6.14 and 1.6.1, by ensuring that additional space is always reserved for each item inserted. The fix also simplified the implementation of `insert_many` to use less unsafe code, so it is easier to verify its correctness.

Thank you to Yechan Bae (@Qwaz) and the Rust group at Georgia Tech's SSLab for finding and reporting this bug.