RUSTSEC-2021-0040

panic safety: double drop or uninitialized drop of T upon panic

Reported	January 12, 2021
Issued	March 7, 2021 (last modified: October 19, 2021)
Package	arenavec (crates.io)
Type	Vulnerability
Categories	memory-corruption
Aliases	CVE-2021-29930 CVE-2021-29931
Details	https://github.com/ibabushkin/arenavec/issues/1
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	no patched versions

Description

Affected versions of this crate did not guard against potential panics that may happen from user-provided functions `T::default()` and `T::drop()`.

Panic within `T::default()` leads to dropping uninitialized `T`, when it is invoked from `common::Slice::<T, H>::new()`. Panic within `T::drop()` leads to double drop of `T`, when it is invoked either from `common::SliceVec::<T, H>::resize_with()` or `common::SliceVec::<T, H>::resize()`

Either case causes memory corruption in the heap memory.