RUSTSEC-2021-0039

panic in user-provided `Endian` impl triggers double drop of T

Reported	January 4, 2021
Issued	March 7, 2021 (last modified: October 19, 2021)
Package	endian_trait (crates.io)
Type	Vulnerability
Categories	memory-corruption
Aliases	CVE-2021-29929
Details	https://gitlab.com/myrrlyn/endian_trait/-/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 the crate does not guard against panic from user-provided impl of `Endian` trait, which is a safe trait that users can implement. If a user-provided implementation of the `Endian` trait panics, double-drop is triggered due to the duplicated ownership of `T` created by `ptr::read()` .

Double-drop (or double free) can cause memory corruption in the heap.