



Look up package or ID...

[About](#) [Advisories](#) [Report Vulnerabilities](#)



## RUSTSEC-2020-0038

[History](#) · [Edit](#)

Memory safety issues in `compact::Vec`

**Reported** September 3, 2020

**Issued** October 2, 2020 (last modified: October 19, 2021)

**Package** [ordnung](#) ([crates.io](#))

**Type** Vulnerability

**Aliases** [CVE-2020-35890](#)  
[CVE-2020-35891](#)

**Details** <https://github.com/maciejhirs/ordnung/issues/8>

**CVSS Score** 7.5 HIGH

### CVSS Details

<b>Attack vector</b>	Network
<b>Attack complexity</b>	Low
<b>Privileges required</b>	None
<b>User interaction</b>	None
<b>Scope</b>	Unchanged
<b>Confidentiality</b>	None
<b>Integrity</b>	None
<b>Availability</b>	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

`compact::Vec` contains multiple memory safety issues.

1. It mishandles large capacity and causes out-of-bound access in 32-bit / allocator layout mismatch in 64-bit.
2. `remove()` is not panic-safe and causes double-free when an index larger than the length is provided.