# RUSTSEC-2021-0070



## VecStorage Deserialize Allows Violation of Length Invariant

| | |
|---|---|
| Reported | June 6, 2021 |
| Issued | June 6, 2021 (last modified: November 6, 2021) |
| Package | nalgebra (crates.io) |
| Type | Vulnerability |
| Categories | memory-corruption<br>memory-exposure |
| Keywords | #memory-safety |
| Aliases | CVE-2021-38190 |
| Details | https://github.com/dimforge/nalgebra/issues/883 |
| Patched | `>=0.27.1` |
| Unaffected | `<0.11.0` |

### Description

The `Deserialize` implementation for `VecStorage` did not maintain the invariant that the number of elements must equal `nrows * ncols`. Deserialization of specially crafted inputs could allow memory access beyond allocation of the vector.

This flaw was introduced in v0.11.0 (`086e6e`) due to the addition of an automatically derived implementation of `Deserialize` for `MatrixVec`. `MatrixVec` was later renamed to `VecStorage` in v0.16.13 (`0f66403`) and continued to use the automatically derived implementation of `Deserialize`.

This flaw was corrected in commit `5bff536` by returning an error during deserialization if the number of elements does not exactly match the expected size.