



Look up package or ID...

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



## RUSTSEC-2021-0011

[History](#) · [Edit](#)

EventList's From conversions can double drop on panic.

Reported	January 4, 2021																
Issued	January 20, 2021 (last modified: October 19, 2021)																
Package	<a href="#">fil-ocl</a> ( <a href="#">crates.io</a> )																
Type	Vulnerability																
Categories	<a href="#">memory-corruption</a>																
Keywords	<a href="#">#memory-safety</a> <a href="#">#double-free</a>																
Aliases	<a href="#">CVE-2021-25908</a>																
Details	<a href="https://github.com/cogciprocate/ocl/issues/194">https://github.com/cogciprocate/ocl/issues/194</a>																
CVSS Score	7.5 HIGH																
CVSS Details	<table><tr><td>Attack vector</td><td>Network</td></tr><tr><td>Attack complexity</td><td>Low</td></tr><tr><td>Privileges required</td><td>None</td></tr><tr><td>User interaction</td><td>None</td></tr><tr><td>Scope</td><td>Unchanged</td></tr><tr><td>Confidentiality</td><td>None</td></tr><tr><td>Integrity</td><td>None</td></tr><tr><td>Availability</td><td>High</td></tr></table>	Attack vector	Network	Attack complexity	Low	Privileges required	None	User interaction	None	Scope	Unchanged	Confidentiality	None	Integrity	None	Availability	High
Attack vector	Network																
Attack complexity	Low																
Privileges required	None																
User interaction	None																
Scope	Unchanged																
Confidentiality	None																
Integrity	None																
Availability	High																
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H</a>																
Patched	no patched versions																
Unaffected	<0.12.0																

### Description

Affected versions of this crate read from a container using `ptr::read` in `From<EventList>`, and then call a user specified `Into<Event>` function.

This issue can result in a double-free if the user provided function panics.