Look up package or ID...

RUSTSEC-2021-0005

History · Edit

Double drop upon panic in 'fn map_array()'

Reported	January 10, 2021
Issued	January 18, 2021 (last modified: October 19, 2021)
Package	glsl-layout (crates.io)
Type	Vulnerability
Categories	memory-corruption
Aliases	CVE-2021-25902
Details	https://github.com/rustgd/glsl-layout/pull/10
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	`>=0.4.0`

Description

Affected versions of this crate did not guard against panic within the user-provided function `f` (2nd parameter of `fn map_array`), and thus panic within `f` causes double drop of a single object.

The flaw was corrected in the 0.4.0 release by wrapping the object vulnerable to a double drop within `ManuallyDrop<T>`.