



Look up package or ID...

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



RUSTSEC-2020-0139

[History](#) · [Edit](#)

dces' World type can cause data races

Reported December 9, 2020

Issued January 30, 2021 (last modified: October 19, 2021)

Package [dces](#) ([crates.io](#))

Type Vulnerability

Categories [memory-corruption](#)
[thread-safety](#)

Keywords [#concurrency](#)

Aliases [CVE-2020-36459](#)

Details <https://gitlab.redox-os.org/redox-os/dces-rust/-/issues/8>

CVSS Score 8.1 HIGH

CVSS Details

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS Vector [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

Patched no patched versions

Description

The `World` type in `dces` is marked as `Send` without bounds on its `EntityStore` and `ComponentStore`.

This allows non-thread safe `EntityStore` and `ComponentStore`s to be sent across threads and cause data races.