



Look up package or ID...

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



## RUSTSEC-2020-0104

[History](#) · [Edit](#)

### ImageChunkMut needs bounds on its Send and Sync traits

**Reported** December 8, 2020

**Issued** January 20, 2021 (last modified: October 19, 2021)

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

**Type** Vulnerability

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

**Aliases** [CVE-2020-36211](#)

**Details** <https://github.com/Devolutions/gfwx-rs/issues/7>

**CVSS Score** 7 HIGH

#### CVSS Details

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

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

**Patched** `>=0.3.0`

#### Description

In the affected versions of this crate, `ImageChunkMut<'_, T>` unconditionally implements `Send` and `Sync`, allowing to create data races.

This can result in a memory corruption or undefined behavior when non thread-safe types are moved and referenced across thread boundaries.

The flaw was corrected in commit `e7fb2f5` by adding `T: Send` bound to the `Send` impl and adding `T: Sync` bound to the `Sync` impl.