Security Advisory for Cargo (CVE-2026-5222)

May 25, 2026 · Rust Security Response Team

The Rust Security Response Team was notified that Cargo incorrectly normalized the URLs of third-party registries using the sparse index protocol. If a hosting provider allowed multiple registries to be hosted with arbitrary names within the same domain, an attacker able to publish crates in a registry could obtain the credentials of others users of the same registry.

This vulnerability is tracked as CVE-2026-5222. The severity of the vulnerability is **low**, due to the extremely niche requirements needed to achieve the attack.

Overview

Originally Cargo only supported storing a registry's index within git repositories. Most git hosting solutions allow accessing a git repository with or without the `.git` suffix, so Cargo mirrored this behavior when normalizing registry URLs. This allowed credentials for `https://example.com/index` to be used for `https://example.com/index.git`.

This normalization was unintentionally applied to the new sparse indexes too. Sparse indexes can be hosted on any HTTPS server, which treat URLs ending with `.git` as different URLs than those without the suffix.

If the following conditions apply:

- `https://example.com/index` is a sparse index.
- `https://example.com/index` allows crates to depend on crates from any other registry.

- The attacker is able to publish crates on `https://example.com/index`.
- The attacker is able to upload arbitrary files to `https://example.com/index.git`.

...the attacker could configure `https://example.com/index.git` to be a Cargo sparse registry requiring authentication for downloads, and with a download URL pointing to a server recording any credentials set to it.

When the attacker then publishes a crate `foo` to `https://example.com/index` depending on a crate `bar` from `https://example.com/index.git`, and tricks the victim into downloading `foo`, Cargo will think the two registries share the same credential and send the victim's Cargo token to the malicious registry.

Mitigations

Rust 1.96, to be released on May 28th, 2026, will update Cargo to only strip the `.git` suffix from registry URLs using the git protocol. No mitigations are available for users of older versions of Cargo.

Affected versions

All versions of Cargo shipped between Rust 1.68 (the stabilization of sparse registries) and 1.96 are affected.

Acknowledgements

We'd like to thank Christos Papakonstantinou for reporting this to us according to the Rust security policy.

We also want to thank the members of the Rust project who helped us address the vulnerability: Arlo Siemens for developing the fix; Weihang Lo, Eric Huss and Emily Albini for reviewing the fix; Emily Albini for writing this advisory; Emily Albini, Josh Stone and Manish Goregaokar for coordinating the disclosure.

Logo Policy and Media Guide

Security Disclosures

All Policies

RSS

Main Blog

"Inside Rust" Blog

Maintained by the Rust Team. See a typo? Send a fix here!