

CVE-2026-32146

Improper Path Validation in Git Dependency Handling Allows Arbitrary File System Modification

[« Back to all CVEs](#)[See on OSV.dev »](#)

Weakness Type (CWE)

[CWE-22 — CWE-22 Improper Limitation of a Pathname to a Restricted Directory \('Path Traversal'\)](#)

CAPEC

[CAPEC-139 — CAPEC-139 Relative Path Traversal](#)[CAPEC-597 — CAPEC-597 Absolute Path Traversal](#)

CVSS 4.0 Score

8.3

HIGH

[CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:N/SC:H/SI:H/SA:H](#)

Vulnerability description

Improper path validation vulnerability in the Gleam compiler's handling of git dependencies allows arbitrary file system modification during dependency download.

Dependency names from `gleam.toml` and `manifest.toml` are incorporated into filesystem paths without sufficient validation or confinement to the intended dependency directory, allowing attacker-controlled paths (via relative traversal such as `../` or absolute paths) to target filesystem locations outside that directory. When resolving git dependencies (e.g. via `gleam deps download`), the computed path is used for filesystem operations including directory deletion and creation.

This vulnerability occurs during the dependency resolution and download phase, which is generally expected to be limited to fetching and preparing dependencies within a confined directory. A malicious direct or transitive git dependency can exploit this issue to delete and overwrite arbitrary directories outside the intended dependency directory, including attacker-chosen absolute paths, potentially causing data loss. In some environments, this may be further leveraged to achieve code execution, for example by overwriting git hooks or shell configuration files.

This issue affects Gleam from 1.9.0-rc1 until 1.15.4.

Affected

pkg:sid/gleam.run/gleam

Module	Source File	Routine
compiler-core	compiler-core/src/config.rs	compiler_core::config::dependencies_map::deserialize
	compiler-core/src/manifest.rs	compiler_core::config::package_name::deserialize

Status	Type	Version	Changes / Fixed in
Affected	semver 	1.9.0-rc1	<ul style="list-style-type: none"> unaffected at 1.15.4

[pkg:github/gleam-lang/gleam](https://github.com/gleam-lang/gleam)

Module	Source File	Routine
compiler-core	compiler-core/src/config.rs	compiler_core::config::dependencies_map::deserialize
	compiler-core/src/manifest.rs	compiler_core::config::package_name::deserialize

Status	Type	Version	Changes / Fixed in
Affected	semver i	1.9.0-rc1	<ul style="list-style-type: none"> unaffected at 1.15.4
Affected	git i	a4fde22445	<ul style="list-style-type: none"> unaffected at 92aae39135 unaffected at 2dc0467f82

[pkg:oci/gleam](https://oci/gleam)

Module	Source File	Routine
compiler-core	compiler-core/src/config.rs	compiler_core::config::dependencies_map::deserialize
	compiler-core/src/manifest.rs	compiler_core::config::package_name::deserialize

Status	Type	Version	Changes / Fixed in
Affected	other	v1.9.0-rc1-elixir	< v1.15.4-elixir
Affected	other	v1.9.0-rc1-erlang	< v1.15.4-erlang
Affected	other	v1.9.0-rc1-node	< v1.15.4-node
Affected	other	v1.9.0-rc1-node-slim	< v1.15.4-node-slim
Affected	other	v1.9.0-rc1-elixir-slim	< v1.15.4-elixir-slim
Affected	other	v1.9.0-rc1-erlang-slim	< v1.15.4-erlang-slim
Affected	other	v1.9.0-rc1-erlang-alpine	< v1.15.4-erlang-alpine
Affected	other	v1.9.0-rc1-elixir-alpine	< v1.15.4-elixir-alpine
Affected	other	v1.9.0-rc1-node-alpine	< v1.15.4-node-alpine
Affected	other	v1.9.0-rc1-scratch	< v1.15.4-scratch

Configurations

The project must use git-based dependencies (direct or transitive), or the victim must run `gleam deps download` on a repository with a malicious `manifest.toml` lockfile. Projects that exclusively use Hex dependencies and do not clone untrusted repositories are not affected.

Projects that exclusively use trusted or personally controlled git dependencies, or dependencies pinned to verified commit SHAs, are not exposed.

Workarounds

- Avoid using untrusted git dependencies, especially without pinning to a specific commit SHA
- Review dependency trees carefully, including transitive git dependencies
- Run dependency resolution commands in a restricted or isolated environment (e.g. containers)

Solutions

Upgrade to Gleam 1.15.4 or later.

Both patches must be applied: the original incomplete fix ([↪ 1aa5d8e594](#), backported as `55bb36e6d7febfbbc48c4d001e0ae13eb0312d78` to 1.15) and the follow-up fix ([↪ 2dc0467f82](#), backported as `92aae3913570e8d8962f6399404777d313045bfa` to 1.15). Gleam 1.15.4 includes both.

References

- <https://github.com/gleam-lang/gleam/security/advisories/GHSA-vq5j-55vx-wq8j> vendor-advisory related
- <https://osv.dev/vulnerability/EEF-CVE-2026-32146> related
- <https://github.com/gleam-lang/gleam/commit/1aa5d8e594b0aa240bb213fce6ee19c65e6d5bcf> patch
- <https://github.com/gleam-lang/gleam/commit/2dc0467f822c75de94697a912755d172928ee40a> patch

Credits

- **Remediation developer:** John Downey
- **Analyst:** Louis Pilfold
- **Coordinator:** Jonatan Männchen / EEF

CVE record as JSON: [GET /cves/CVE-2026-32146.json](#)

OSV record as JSON: [GET /osv/EEF-CVE-2026-32146.json](#)



ERLANG ECOSYSTEM
FOUNDATION

Supporting the BEAM community

ABOUT THE EEF

[Membership details](#)

[Join us!](#)

[Sponsors](#)

[Working Groups](#)

[Stipends](#)

[Bylaws](#)

[FAQ](#)

STAY UP-TO-DATE

[News](#)

[Events](#)

GET IN TOUCH

[Contact Us](#)

