fix: sanitize inspect output path #4793

Merged AustinAbro321 merged 2 commits into `main` from `sanitaize-name-path` last week

AustinAbro321 commented last week • edited — Member

Description

This prevents package name that's been edited to go an arbitrary directory from leaving the cwd when using `zarf package inspect definition` or `zarf package inspect sbom`

Checklist before merging

- [ ] Test, docs, adr added or updated as needed
- [ ] Contributor Guide Steps followed

`sanitize path` ··· ✓ `48722af`

AustinAbro321 requested review from **a team** as code owners last week

github-project-automation bot added this to **Zarf** last week

netlify bot commented last week • edited

✅ Deploy Preview for *zarf-docs* canceled.

Name	Link
🔨 Latest commit	`9c9f43e`
🔍 Latest deploy log	https://app.netlify.com/projects/zarf-docs/deploys/69d68c59c9f15b0008bf4526

codecov bot commented last week • edited

Codecov Report

❌ Patch coverage is `50.00000%` with `3 lines` in your changes missing coverage. Please review.

Files with missing lines	Patch %	Lines
src/pkg/packager/create.go	0.00%	2 Missing ⚠️
src/cmd/package.go	50.00%	1 Missing ⚠️

Files with missing lines	Coverage Δ	
src/pkg/packager/layout/package.go	`65.01% <100.00%> (+0.13%)`	⬆️
src/cmd/package.go	`38.08% <50.00%> (ø)`	
src/pkg/packager/create.go	`55.31% <0.00%> (-0.60%)`	⬇️

... and 3 files with indirect coverage changes

▶ 🚀 New features to boost your workflow:

dgershman previously approved these changes last week

View reviewed changes

dgershman left a comment Contributor

Code & Security Review

Critical Issues

None.

Security Review

Strengths:

- Correctly fixes a path traversal vulnerability where a maliciously crafted package name (e.g., `../../etc/evil`) could write SBOM or documentation files outside the intended output directory.
- `filepath.Base()` is the right mitigation — it strips all directory components, preventing traversal while preserving the actual name.
- Fix is applied consistently across all three affected call sites:
  - `src/cmd/package.go` — SBOM inspect output path
  - `src/cmd/package.go` — documentation inspect output path
  - `src/pkg/packager/create.go` — SBOM output during package create

Minor Observation:

- `filepath.Base("")` returns `"."`, which would produce an output path like `outputDir/.` — but an empty package name is an edge case that would likely be caught by other validation. Not a blocking issue.
- No test is added for the sanitization. A unit test verifying that a name like `../../traversal` is sanitized to `traversal` would strengthen confidence, but the fix itself is straightforward enough that this isn't blocking.

Code Quality

- Clean, minimal change with appropriate comments explaining the "why."
- No unnecessary refactoring.

Summary Table

Priority	Issue
🟢 Green	Consider adding a test for path traversal sanitization
🟢 Green	Edge case: empty package name produces `"."` via `filepath.Base("")` (unlikely in practice)

Recommendation: Approve — the fix is correct, minimal, and consistently applied across all affected paths.

AustinAbro321 added this pull request to the merge queue last week

AustinAbro321 removed this pull request from the merge queue due to a manual request last week

View details

`sanatize layout` ··· `9c9f43e`

AustinAbro321 dismissed **dgershman**'s stale review via `9c9f43e` last week

brandtkeller approved these changes last week

View reviewed changes

brandtkeller left a comment — Member

lgtm

AustinAbro321 added this pull request to the merge queue last week

github-merge-queue bot removed this pull request from the merge queue due to failed status checks last week

View details

AustinAbro321 added this pull request to the merge queue last week

Merged via the queue into `main` with commit **`abd00af`** last week

32 checks passed

View details

AustinAbro321 deleted the `sanitaize-name-path` branch last week

github-project-automation bot moved this to **Done** in **Zarf** last week

zarf-release-please bot mentioned this pull request last week

chore(main): release 0.74.2 #4802

Merged

Reviewers

 **brandtkeller** ✓

 **dgershman**

Assignees

No one assigned

Labels

None yet

Projects

Zarf

Status: Done +5 more

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants