Path traversal in melange's external pipeline resolver (pipeline[].uses) allows loading a pipeline from outside the pipeline directories

Moderate **antitree** published **GHSA-98f2-w9h9-7fp9** 3 days ago

Package

melange (Go)

Affected versions	Patched versions
>= 0.32.0, < 0.43.4	0.43.4

Description

Impact

An attacker who can influence a melange configuration file — for example through pull-request-driven CI or build-as-a-service scenarios — could set `pipeline[].uses` to a value containing `../` sequences or an absolute path. The `(*Compiled).compilePipeline` function in `pkg/build/compile.go` passed `uses` directly to `filepath.Join(pipelineDir, uses + ".yaml")` without validating the value, so the resolved path could escape each `--pipeline-dir` and read an arbitrary YAML-parseable file visible to the melange process. Because the loaded file is subsequently interpreted as a melange pipeline and its `runs:` block is executed via `/bin/sh -c` in the build sandbox, this additionally allowed shell commands sourced from an out-of-tree file to run during the build, bypassing the review boundary that normally covers the in-tree pipeline definition.

Patches

Fixed in melange **v0.43.4** via commit 5829ca4. The fix rejects `uses` values that are absolute paths or contain `..`, and verifies (via `filepath.Rel` after `filepath.Clean`) that the resolved target remains within the pipeline directory.

Workarounds

Only run `melange build` against configuration files from trusted sources. In CI systems that build user-supplied melange configs, gate builds behind manual review of `pipeline[].uses` values and reject any containing `..` or leading `/`.

References

- `5829ca4`

Credits

Thank you to Oleh Konko (@1seal from 1seal.org) for discovering and reporting this issue.

Severity

Moderate 6.1 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	Low
Availability	None

Learn more about base metrics

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N

CVE ID

CVE-2026-29050

Weaknesses

▶ CWE-22

Credits

1seal	Reporter
antitree	Analyst