Path traversal in melange --persist-lint-results via unvalidated .PKGINFO fields

Moderate **antitree** published **GHSA-q2pw-xx38-p64j** 3 days ago

Package

melange (Go)

Affected versions

>= 0.32.0, < 0.43.4

Patched versions

0.43.4

Description

Impact

`melange lint --persist-lint-results` (opt-in flag, also usable via `melange build --persist-lint-results`) constructs output file paths by joining `--out-dir` with the `arch` and `pkgname` values read from the `.PKGINFO` control file of the APK being linted. In affected versions these values were not validated for path separators or `..` sequences, so an attacker who can supply an APK to a melange-based lint/build pipeline (e.g. CI that lints third-party APKs, or build-as-a-service) could cause melange to write `lint-<pkgname>-<pkgver>-r<epoch>.json` to an arbitrary `.json` path reachable by the melange process. The written file is a JSON lint report whose content is partially attacker-influenced. There is no direct code-execution path, but the write can clobber other JSON artifacts on the filesystem. The issue only affects deployments that explicitly pass `--persist-lint-results`; the flag is off by default.

Patches

Fixed in melange **v0.43.4** by validating `arch` and `pkgname` for `..`, `/`, and `filepath.Separator` before path construction in `pkg/linter/results.go` (commit 84f3b45).

Workarounds

Do not pass `--persist-lint-results` when linting or building APKs whose `.PKGINFO` contents are not fully trusted. Running melange as a low-privileged user and confining writes to an isolated directory also limits impact.

References

- `84f3b45`

Credits

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

Severity

Moderate 4.4 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-29051

Weaknesses

▶ CWE-22

Credits

1seal	Reporter
antitree	Analyst