`cosign verify-attestation --type` can report a false positive if any attestation exists

Moderate **priyawadhwa** published **GHSA-vjxv-45g9-9296** on Aug 4

Package

cosign (cosign)

Affected versions	Patched versions
< 1.10.0	1.10.1

Description

Impact

`cosign verify-attestation` used with the `--type` flag will report a false positive verification when:

- There is at least one attestation with a valid signature
- There are NO attestations of the type being verified (--type defaults to "custom")

This can happen when signing with a standard keypair and with "keyless" signing with Fulcio.

Reproduce

This vulnerability can be reproduced with the `distroless.dev/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e2` image.

This image has a `vuln` attestation but not an `spdx` attestation.
However, if you run `cosign verify-attestation --type=spdx` on this image, it incorrectly succeeds:

```
COSIGN_EXPERIMENTAL=true cosign verify-attestation --type spdx
distroless.dev/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e2
```

To see the predicate type:

```
# Get the predicate type
COSIGN_EXPERIMENTAL=true cosign verify-attestation --type spdx
distroless.dev/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e2
| jq -r .payload | base64 -d | jq -r .predicateType

cosign.sigstore.dev/attestation/vuln/v1
```

Patches

Users should upgrade to cosign version 1.10.1 or greater for a patch.

Workarounds

Currently the only workaround is to upgrade.

For more information

If you have any questions or comments about this advisory:

- Open an issue in cosign
- Send us a message on Slack. Invite link here.

Thank you

Thank you to **@mattmoor** for finding and reporting this vulnerability.

Severity

Moderate

CVE ID

CVE-2022-35929

Weaknesses

No CWEs