<> **Code**   ⊙ **Issues** 163   ⑂ **Pull requests** 14   🗩 **Discussions**   ⊙ **Actions**   •••

✕ **Merge pull request from GHSA-vjxv-45g9-9296**   **Browse files**

```
     Today the verification logic:
 1. Verifies signatures on attestations (at least one must verify, or it errors),
 2. All attestations matching the specified `--type` must pass any specified Cue/Rego policies,
 3. *All* signature-verified attestations are then printed.

 However, if NONE of the attestations match the specified `--type` then `2.` is considered
 satisfied and we proceed to `3.`

 This changes the above logic to:
 1. Same.
 2. Same, but these are put into a `checked` list,
 3. `checked` must be non-empty (or an error is printed about no attestations matching `--type`),
 4. *Just* the `checked` attestations are printed.

 ---

 The bug at HEAD:
 ```shell
 $ cosign verify-attestation --type spdx
 ghcr.io/distroless/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e
 2

 Verification for
 ghcr.io/distroless/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e
 2 --
 The following checks were performed on each of these signatures:
   - The cosign claims were validated
   - Existence of the claims in the transparency log was verified offline
   - Any certificates were verified against the Fulcio roots.
 Certificate subject:
 https://github.com/distroless/static/.github/workflows/release.yaml@refs/heads/main
 Certificate issuer URL:   https://token.actions.githubusercontent.com
 Certificate extension GitHub Workflow Trigger: schedule
 Certificate extension GitHub Workflow SHA: 7e7572e578de7c51a2f1a1791f025cf315503aa2
 Certificate extension GitHub Workflow Name: Create Release
 Certificate extension GitHub Workflow Trigger distroless/static
 Certificate extension GitHub Workflow Ref: refs/heads/main
```
{"payloadType":"application/vnd.in-
toto+json","payload":"eyJfdHlwZSI6Imh0dHBzOi8vaW4tdG90by5pby9TdGF0ZW1lbnQvdjAuMSIsInByZWRpY2F0ZV
R5cGUiOiJjb3NpZ24uc2lnc3RvcmUuZGV2L2F0dGVzdGF0aW9uL3Z1bG4vdjEiLCJzdWJqZWN0IjpbeyJuYW1lIjoiZ2hjci
5pby9kaXN0cm9sZXNzL3N0YXRpYyIsImRpZ2VzdCI6eyJzaGEyNTYiOiJkZDc2MTRiNWExMmJjNGQ2MTdiMjIzYzU4OGI0ZT
BjODMzNDAyYjhmNDk5MWZiNTcwMmVhODNhZmFkMTk4NmUyIn19XSwicHJlZGljYXRlIjp7Imludm9jYXRpb24iOnsiY2FyYW
1ldGVycyI6bnVsbCwidXJpIjoiaHR0cHM6Ly9naXRodWIuY29tL2Rpc3Ryb2xlc3Mvc3RhdGljL2FjdGlvbnMvcnVucy8yNz
```

c5MjEyNzA1IiwiZXZlbnRfaWQiOiIyNzc5MjEyNzA1IiwiYnVpbGRlci5pZCI6IkNyZWF0ZSBSZWxlYXNlIn0sInNjYW5uZX
IiOnsidXJpIjoiaHR0cHM6Ly9naXRodWIuY29tL2FxdWFzZWN1cml0eS90cml2eSIsInZlcnNpb24iOiIwLjI5LjIiLCJkYi
I6eyJ1cmkiOiIiLCJ2ZXJzaW9uIjoiIn0sInJlc3VsdCI6eyIkc2NoZW1hIjoiaHR0cHM6Ly9qc29uLnNjaGVtYXN0b3JlLm
9yZy9zYXJpZi0yLjEuMC1ydG0uNS5qc29uIiwicnVucyI6W3siY29udGVudHMiZCI6InV0ZjE2Q29kZVVuaXRzIiwib3JpZ2
luYWxVcmlCYXNlSWRzIjp7IlJPT1RQQVRII6p7InVyaSI6ImZpbGU6Ly8vIn19LCJyZXN1bHRzIjpbXSwidG9vbCI6eyJkcm
l2ZXIiOnsiZnVsbE5hbWUiOiJUcml2eSBWdWxuZXJhYmlsaXR5IFNjYW5uZXIiLCJpbmZvcm1hdGlvblVyaSI6Imh0dHBzOi
8vZ2l0aHViLmNvbS9hcXVhc2VjdXJpdHkvdHJpdmkiLCJuYW1lIjoiVHJpdmkiLCJydWxlcyI6W10sInZlcnNpb24iOiIwLj
I5LjIifX19XSwidmVyc2lvbiI6IjIuMS4wIn19LCJtZXRhZGF0YSI6eyJzY2FuU3RhcnRlZE9uIjoiMjAyMi0wOC0wMlQwMj
ozMzo0N1oiLCJzY2FuRmluaXNoZWRPbiI6IjIwMjItMDgtMDJUMDI6MzM6NTNaIn19fQ==","signatures":
[{"keyid":"","sig":"MEYCIQCovBtLOBXyB2zpvhp3j6QzqLtsH0/RC7fRINSApySqxAIhAIKlzu1fXuKPPOIheNnsPmBO
B6XfZbRs5sDW1yFSch1A"}]}
```

The same with this change:
```shell
$ go run ./cmd/cosign verify-attestation --type spdx
ghcr.io/distroless/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e
2
Error: none of the attestations matched the predicate type: spdx
main.go:62: error during command execution: none of the attestations matched the predicate type:
spdx
exit status 1
```

A valid `--type` with this change:
```shell
$ go run ./cmd/cosign verify-attestation --type vuln
ghcr.io/distroless/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e
2

Verification for
ghcr.io/distroless/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e
2 --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - Existence of the claims in the transparency log was verified offline
  - Any certificates were verified against the Fulcio roots.
Certificate subject:
https://github.com/distroless/static/.github/workflows/release.yaml@refs/heads/main
Certificate issuer URL:  https://token.actions.githubusercontent.com
Certificate extension GitHub Workflow Trigger: schedule
Certificate extension GitHub Workflow SHA: 7e7572e578de7c51a2f1a1791f025cf315503aa2
Certificate extension GitHub Workflow Name: Create Release
Certificate extension GitHub Workflow Trigger distroless/static
Certificate extension GitHub Workflow Ref: refs/heads/main
```

{"payloadType":"application/vnd.in-
toto+json","payload":"eyJfdHlwZSI6Imh0dHBzOi8vaW4tdG90by5pby9TdGF0ZW1lbnQvdjAuMSIsInByZWRpY2F0ZV
R5cGUiOiJjb3NpZ24uc2lnc3RvcmUuZGV2L2F0dGVzdGF0aW9uL3Z1bG4vdjEiLCJzdWJqZWN0IjpbeyJuYW1lIjoiZ2hjci
5pby9kaXN0cm9sZXNzL3N0YXRpYyIsImRpZ2VzdCI6eyJzaGEyNTYiOiJkZDc2MTRiNWExMmJjNGQ2MTdiMjIzYzU4OGI0ZT
BjODMzNDAyYjhmNDk5MWZiNTcwMmVhODNhZmFkMTk4NmUyIn19XSwicHJlZGljYXRlIjp7Imludm9jYXRpb24iOnsicGFyYW
1ldGVycyI6bnVsbCwidXJpIjoiaHR0cHM6Ly9naXRodWIuY29tL2Rpc3Ryb2xlc3Mvc3RhdGljL2FjdGlvbnMvcnVucy8yNz
c5MjEyNzA1IiwiZXZlbnRfaWQiOiIyNzc5MjEyNzA1IiwiYnVpbGRlci5pZCI6IkNyZWF0ZSBSZWxlYXNlIn0sInNjYW5uZX

IiOnsidXJpIjoiaHR0cHM6Ly9naXRodWIuY29tL2FxdWFzZWN1cml0eS90cml2eSIsInZlcnNpb24iOiIwLjI5LjIiLCJkYi
I6eyJ1cmkiOiIiLCJ2ZXJzaW9uIjoiIn0sInJlc3VsdCI6eyIkc2NoZW1hIjoiaHR0cHM6Ly9qc29uLnNjaGVtYXN0b3JlLm
9yZy9zYXJpZi0yLjEuMC1ydG0tNS5qc29uIiwicnVucyI6W3siY29sdW1uS2luZCI6InV0ZjE2Q29kZVVuaXRzIiwib3JpZ2
luYWxVcmlCYXNlSWRzIjp7IlJPT1RQQVRII jp7InVyaSI6ImZpbGU6Ly8vIn19LCJyZXN1bHRzIjpbXSwidG9vbCI6eyJkcm
l2ZXIiOnsiZnVsbE5hbWUiOiJUcml2eSBWdWxuZXJhYmlsaXR5IFNjYW5uZXIiLCJpbmZvcm1hdGlvblVyaSI6Imh0dHBzOi
8vZ2l0aHViLmNvbS9hcXVhc2VjdXJpdHkvdHJpdnkiLCJuYW1lIjoiVHJpdnkiLCJydWxlcyI6W10sInZlcnNpb24iOiIwLj
I5LjIifX19XSwidmVyc2lvbiI6IjIuMS4wIn19LCJtZXRhZGF0YSI6eyJzY2FuU3RhcnRlZ9uIjoiMjAyMi0wOC0wMlQwMj
ozMzo0N1oiLCJzY2FuRmluaXNoZWRPbiI6IjIwMjItMDgtMDJUMDI6MzM6NTNaIn19fQ==","signatures":
[{"keyid":"","sig":"MEYCIQCovBtLOBXyB2zpvhp3j6QzqLtsH0/RC7fRINSApySqxAIhAIKlzu1fXuKPPOIheNnsPmBO
B6XfZbRs5sDW1yFSch1A"}]}
```

Signed-off-by: Matt Moore <mattmoor@chainguard.dev>

⑂ **main**

◇ **v1.13.1** ... v1.10.1

👤 **mattmoor** committed on Aug 4 ┃ parent 641f02b   commit c5fda01a8ff33ca981f45a9f13e7fb6bd2080b94

Showing **1 changed file** with **10 additions** and **1 deletion**.   Split   Unified

---

∨ ⋮⋮ 11 ■■■■□ cmd/cosign/cli/verify/verify_attestation.go 🗐

201	201		}
202	202		}
203	203		
	204	+	var checked []oci.Signature
204	205		var validationErrors []error
205	206		for _, vp := range verified {
206	207		payload, err := policy.AttestationToPayloadJSON(ctx, c.PredicateT
217	218		cueValidationErr := cue.ValidateJSON(payload, cuePolicies
218	219		if cueValidationErr != nil {
219	220		validationErrors = append(validationErrors, cueVa
	221	+	continue
220	222		}
221	223		}
222	224		
225	227		regoValidationErrs := rego.ValidateJSON(payload, regoPoli
226	228		if len(regoValidationErrs) > 0 {
227	229		validationErrors = append(validationErrors, regoV
	230	+	continue
228	231		}
229	232		}
	233	+	
	234	+	checked = append(checked, vp)
230	235		}
231	236		
232	237		if len(validationErrors) > 0 {

```
237    242                              return fmt.Errorf("%d validation errors occurred", len(validation
238    243                          }
239    244
       245    +                      if len(checked) == 0 {
       246    +                          return fmt.Errorf("none of the attestations matched the predicate
       247    +                      }
       248    +
240    249                          // TODO: add CUE validation report to `PrintVerificationHeader`.
241    250                          PrintVerificationHeader(imageRef, co, bundleVerified, fulcioVerified)
242    251                          // The attestations are always JSON, so use the raw "text" mode for outpu
243         -                       PrintVerification(imageRef, verified, "text")
       252    +                      PrintVerification(imageRef, checked, "text")
244    253                      }
245    254
246    255                  return nil
```

◀ ▶

0 comments on commit c5fda01