dapr / **dashboard** Public

Code Issues 30 Pull requests 19 Actions Projects Security ···

New issue Jump to bottom

Vulnerabilities exist for unauthorized access to sensitive information and application closure #222

Open **andrewgogogo** opened this issue on Sep 28 · 0 comments

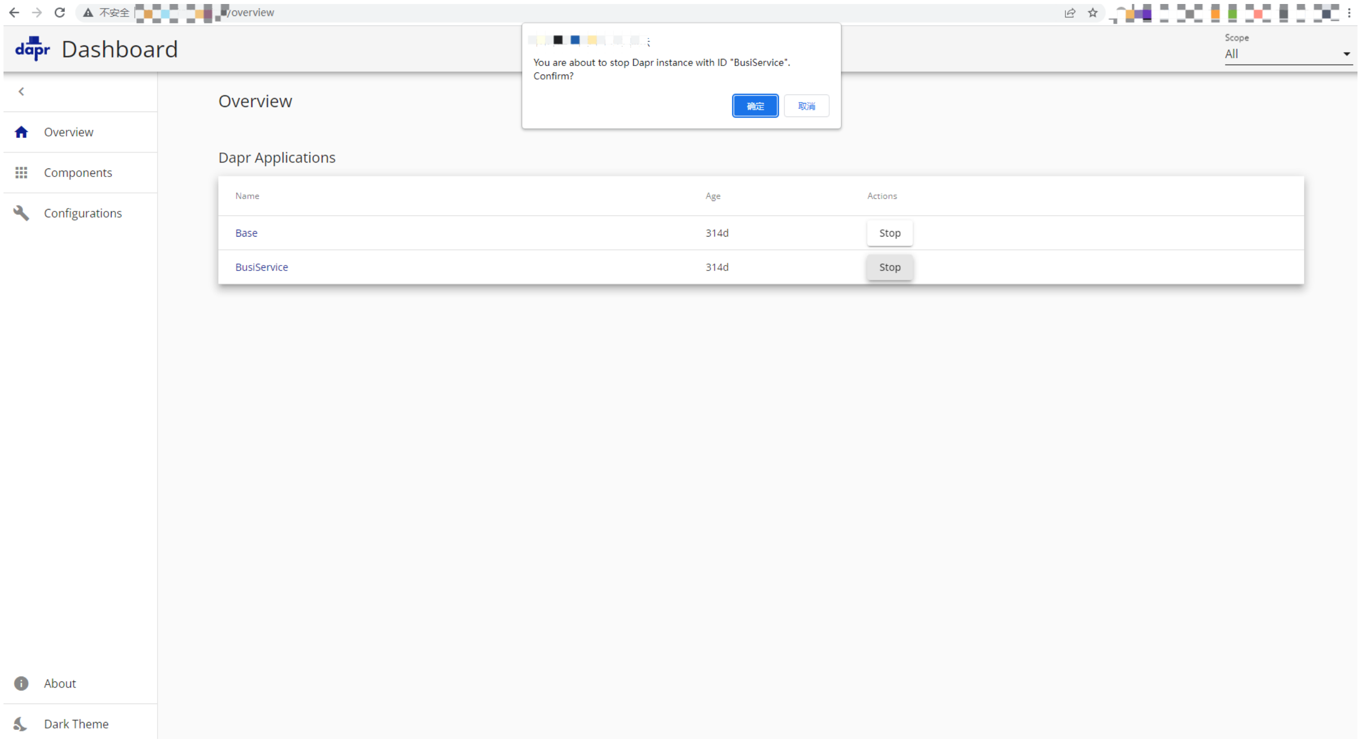
Labels kind/bug

andrewgogogo commented on Sep 28

Detail

According to analysis and research, malicious attackers can use this unauthorized access vulnerability to obtain plaintext configuration information of redis, mongodb, rabbitmq and other applications on the cloud without authorization, and can further use these configuration information to obtain sensitive data on the cloud. In addition, the Dapr Dashboard configured with the Actions option (v0.2.0 verified) can be closed by a malicious attacker without authorization, causing business interruption.

Example



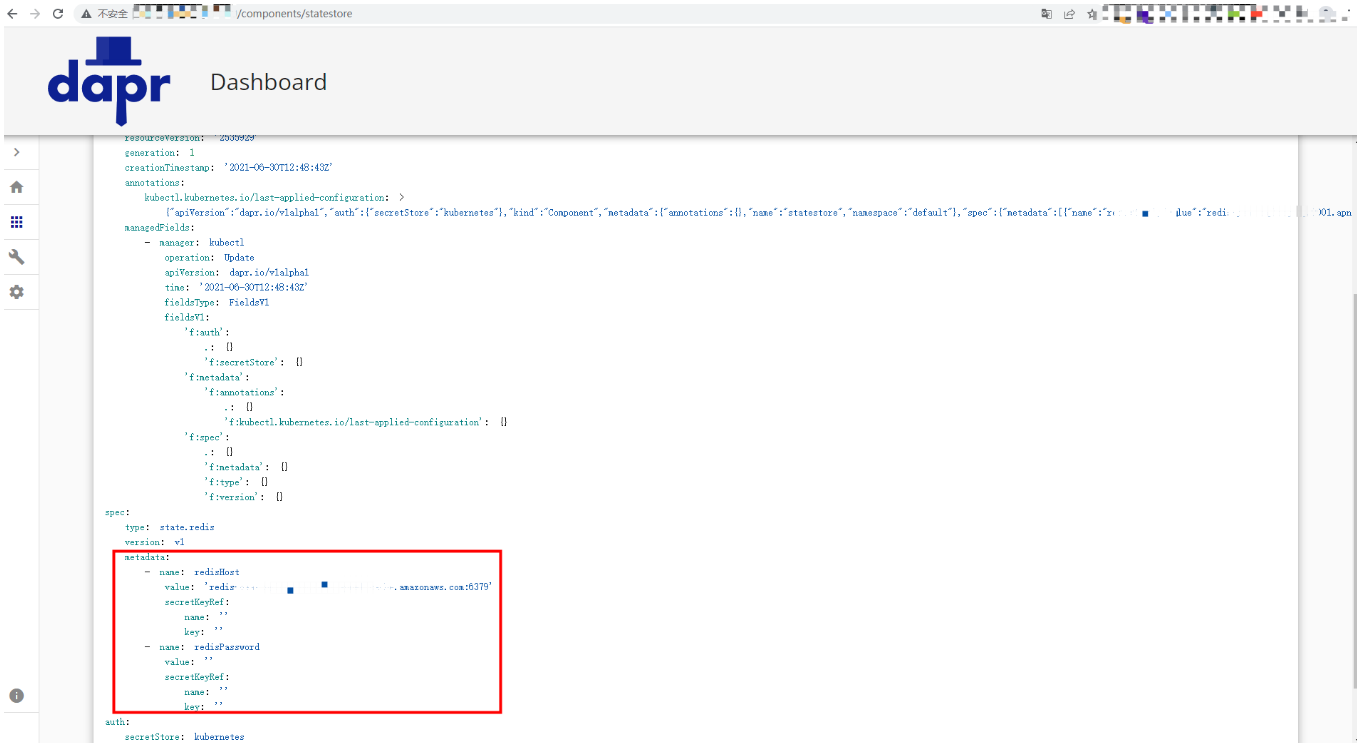
[redacted]

You are about to stop Dapr instance with ID "BusiService". Confirm?

Overview

Dapr Applications

Name	Age	Actions
Base	314d	Stop
BusiService	314d	Stop



```
    resourceVersion: '2535929'
    generation: 1
    creationTimestamp: '2021-06-30T12:48:43Z'
    annotations:
        kubectl.kubernetes.io/last-applied-configuration: >
            {"apiVersion":"dapr.io/v1alpha1","auth":{"secretStore":"kubernetes"},"kind":"Component","metadata":{"annotations":{},"name":"statestore","namespace":"default"},"spec":{"metadata":[{"name":"re[redacted]lue":"redi[redacted]001.apn
    managedFields:
        - manager: kubectl
          operation: Update
          apiVersion: dapr.io/v1alpha1
          time: '2021-06-30T12:48:43Z'
          fieldsType: FieldsV1
          fieldsV1:
              'f:auth':
                  .: {}
                  'f:secretStore': {}
              'f:metadata':
                  'f:annotations':
                      .: {}
                      'f:kubectl.kubernetes.io/last-applied-configuration': {}
              'f:spec':
                  .: {}
                  'f:metadata': {}
                  'f:type': {}
                  'f:version': {}
spec:
    type: state.redis
    version: v1
    metadata:
        - name: redisHost
          value: 'redis-[redacted].amazonaws.com:6379'
          secretKeyRef:
              name: ''
              key: ''
        - name: redisPassword
          value: ''
          secretKeyRef:
              name: ''
              key: ''
auth:
    secretStore: kubernetes
```

Repair

Temporary Mitigation: Strict whitelist access controls can be applied to affected assets.
Solution: Add login authentication for Dapr Dashboard.

andrewgogogo added the kind/bug label on Sep 28

GoVulnBot mentioned this issue on Oct 3

x/vulndb: potential Go vuln in github.com/dapr/dashboard: CVE-2022-38817
golang/vulndb#1033

Closed

Assignees

No one assigned

Labels

kind/bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant