

[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

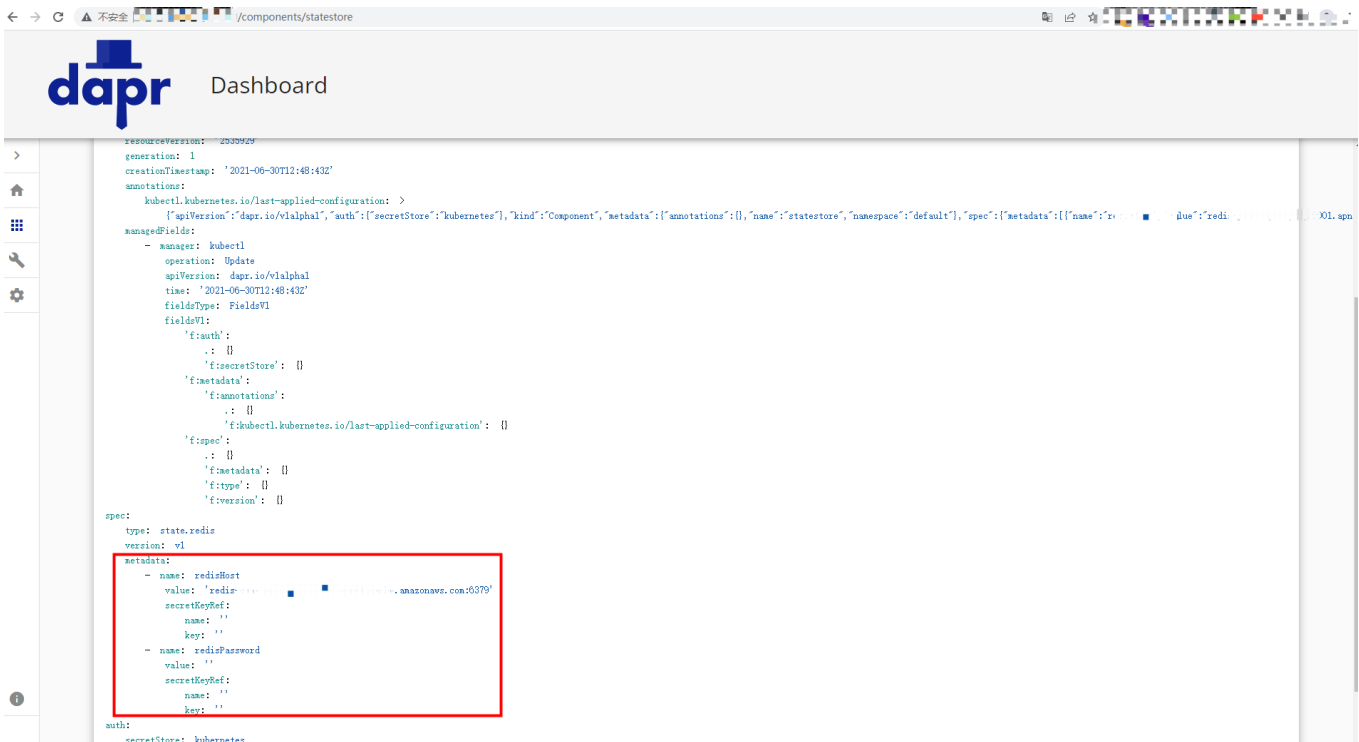
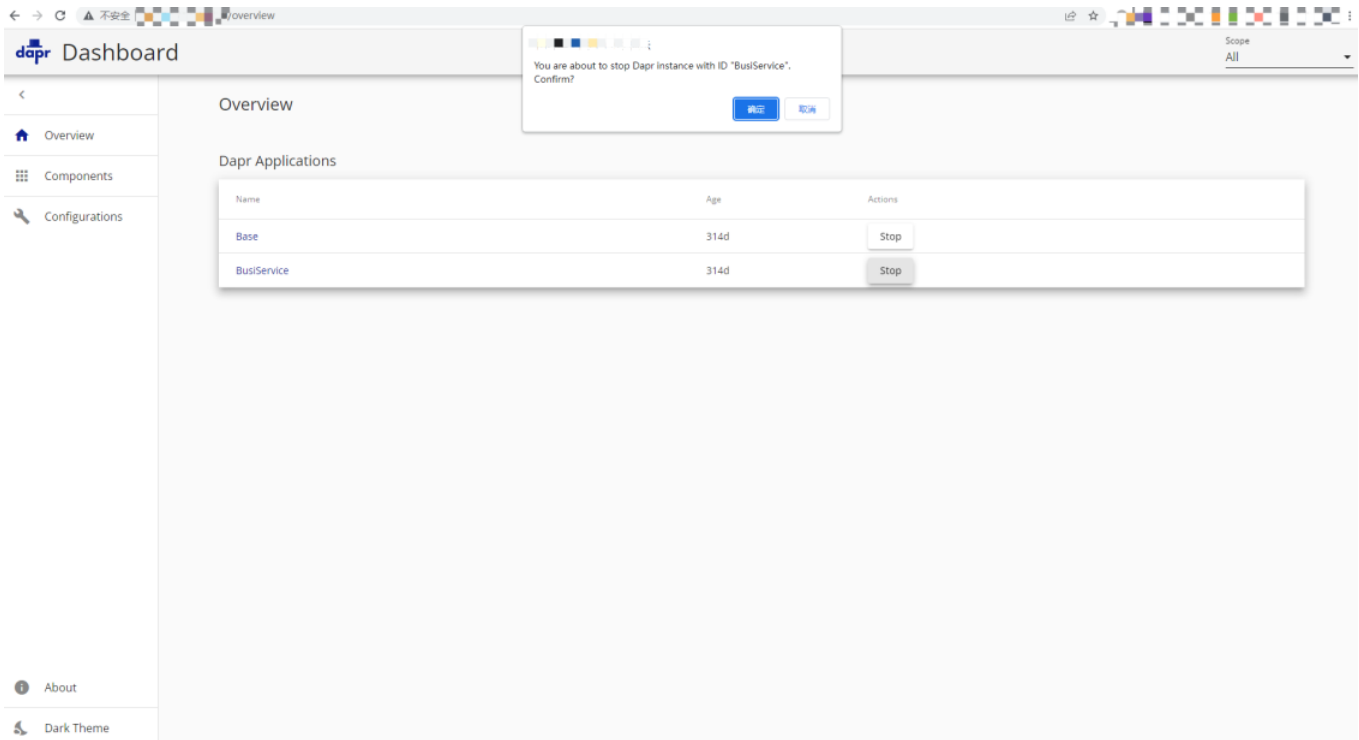
kind/bug

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



Repair

Temporary Mitigation: Strict whitelist access controls can be applied to affected assets.

Solution: Add login authentication for Dapr Dashboard.



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

