


# Exposure of server configuration

High wass3r published GHSA-gv2h-gf8m-r68j on Dec 30, 2020

Package

 **compiler** (Go)

Affected versions

< 0.6.1

Patched versions

0.6.1

## Description

### Impact

*What kind of vulnerability is it? Who is impacted?*

- The ability to expose configuration set in the [Vela server](#) via pipeline template functionality.
- It impacts all users of Vela.

Sample of template exposing server configuration using Sprig's `env` function:

```
metadata:
  template: true

steps:
- name: sample
  image: alpine:latest
  commands:
    # OAuth client ID for Vela <-> GitHub communication
    - echo {{ env "VELA_SOURCE_CLIENT" }}
    # secret used for server <-> worker communication
    - echo {{ env "VELA_SECRET" }}
```

### Patches

*Has the problem been patched? What versions should users upgrade to?*

- Upgrade to `0.6.1`

### Additional Recommended Action(s)

- Rotate all secrets

### Workarounds

*Is there a way for users to fix or remediate the vulnerability without upgrading?*

- No

### References

*Are there any links users can visit to find out more?*

- <https://golang.org/pkg/text/template/>
- <https://masterminds.github.io/sprig/os.html>
- <https://go-vela.github.io/docs/templates/overview/>
- <https://github.com/helm/helm/blob/6297c021cbda1483d8c08a8ec6f4a99e38be7302/pkg/engine/funcs.go#L46-L47>

### For more information

If you have any questions or comments about this advisory:

- Email us at [vela@target.com](mailto:vela@target.com)

## Severity

High


## CVE ID

CVE-2020-26294

## Weaknesses

No CWEs

## Credits

 [matt-fevold](#)

 [wass3r](#)