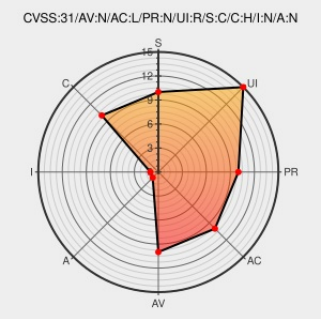
CVE-2020-26294

Published on: 01/04/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:55 PM UTC

CVE-2020-26294 - advisory for GHSA-gv2h-gf8m-r68j

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Compiler from Target contain the following vulnerability:

Vela is a Pipeline Automation (CI/CD) framework built on Linux container technology written in Golang. In Vela compiler before version 0.6.1 there is a vulnerability which allows exposure of server configuration. It impacts all users of Vela. An attacker can use Sprig's `env` function to retrieve configuration information, see referenced GHSA for an example. This has been fixed in version 0.6.1. In addition to upgrading, it is recommended to rotate all secrets.

CVE-2020-26294 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **go-vela** - **compiler** version **< 0.6.1**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Exposure of server configuration · Advisory · go-vela/compiler · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/go-vela/compiler/security/advisories/GHSA-gv2h-gf8m-r68j
fix: disallow functions (#93) · go-vela/compiler@f1ace5f · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/go-vela/compiler/commit/f1ace5f8a05c95c4d02264556e38a959ee2d9bda
compiler · pkg.go.dev	Product Third Party Advisory pkg.go.dev text/html	MISC pkg.go.dev/github.com/go-vela/compiler/compiler

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Target	Compiler	All	All	All	All
Application	Target	Compiler	All	All	All	All

cpe:2.3:a:target:compiler:*:*:*:*:*:*:*:*:

cpe:2.3:a:target:compiler:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→