

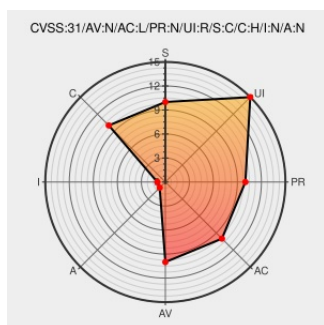


CVE-2020-26294

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

Exposure of server configuration · Advisory · go-vela/compiler · GitHub

Tags

Exploit

Third Party Advisory

github.com

text/html

Link

 CONFIRM github.com/go-vela/compiler/security/advisories/GHSA-gv2h-gf8m-r68j

Description

fix: disallow functions (#93) · go-vela/compiler@f1ace5f · GitHub

Tags

Patch

Third Party Advisory

github.com

text/html

Link

 MISC github.com/go-vela/compiler/commit/f1ace5f8a05c95c4d02264556e38a959ee2d9bda

Description

compiler · pkg.go.dev

Tags

Product

Third Party Advisory

pkg.go.dev

text/html

Link

 MISC pkg.go.dev/github.com/go-vela/compiler/compiler

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 →

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)