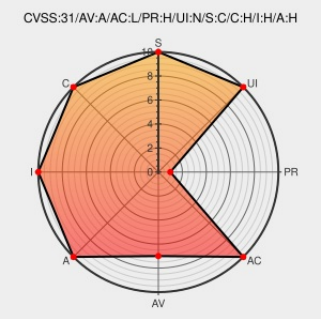
CVE-2021-43837

Published on: Not Yet Published

Last Modified on: 08/09/2022 01:23:00 PM UTC

CVE-2021-43837 - advisory for GHSA-q34h-97wf-8r8j

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



Certain versions of Vault-cli from Ukg contain the following vulnerability:

vault-cli is a configurable command-line interface tool (and python library) to interact with Hashicorp Vault. In versions before 3.0.0 vault-cli features the ability for rendering templated values. When a secret starts with the prefix `!template!`, vault-cli interprets the rest of the contents of the secret as a Jinja2 template. Jinja2 is a powerful templating engine and is not designed to safely render arbitrary templates. An attacker controlling a jinja2 template rendered on a machine can trigger arbitrary code, making this a Remote Code Execution (RCE) risk. If the content of the vault can be completely trusted, then this is not a problem. Otherwise, if your threat model includes cases where an attacker can manipulate a secret value read from the vault using vault-cli, then this vulnerability may impact you. In 3.0.0, the code related to interpreting vault templated secrets has been removed entirely. Users are advised to upgrade as soon as possible. For users unable to upgrade a workaround does exist. Using the environment variable `VAULT_CLI_RENDER=false` or the flag `--no-render` (placed between `vault-cli` and the subcommand, e.g. `vault-cli --no-render get-all`) or adding `render: false` to the vault-cli configuration yaml file disables rendering and removes the vulnerability. Using the python library, you can use: `vault_cli.get_client(render=False)` when creating your client to get a client that will not render templated secrets and thus operates securely.

CVE-2021-43837 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **peopledoc** - **vault-cli** version **>= 0.7.0,< 3.0.0**

CVSS3 Score: 9.1 - CRITICAL

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

Impact	Impact	Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Merge pull request #198 from peopledoc/templates · peopledoc/vault-cli@3ba3955 · GitHub	github.com text/html	MISC github.com/peopledoc/vault-cli/commit/3ba3955887fd6b7d4d646c8b260f21cebf5db852
GreHack 2021 - Optimizing Server Side Template Injections payloads for jinja2 · Podalirius	podalirius.net text/html	MISC podalirius.net/en/publications/grehack-2021-optimizing-ssti-payloads-for-jinja2/
vault-cli: possible RCE when reading user-defined data · Advisory · peopledoc/vault-cli · GitHub	github.com text/html	CONFIRM github.com/peopledoc/vault-cli/security/advisories/GHSA-q34h-97wf-8r8j

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	Ukg	Vault-cli	All	All	All	All
Application	Vault-cli Project	Vault-cli	All	All	All	All

cpe:2.3:a:ukg:vault-cli:*:*:*:*:*:python:*:*

cpe:2.3:a:vault-cli_project:vault-cli:*:*:*:*:*:python:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43837 : vault-cli is a configurable command-line interface tool and python library to interact with Hash… twitter.com/i/web/status/1…	2021-12-16 18:59:20
/r/netcve	CVE-2021-43837	2021-12-16 20:38:11

← 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 registred 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