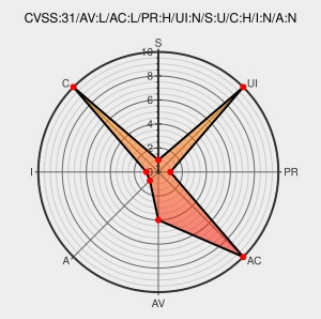
CVE-2021-32638

Published on: 05/25/2021 12:00:00 AM UTC

Last Modified on: 07/02/2022 08:01:00 PM UTC

CVE-2021-32638 - advisory for GHSA-g36v-2xff-pv5m

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



Certain versions of Codeql Action from Github contain the following vulnerability:

Github's CodeQL action is provided to run CodeQL-based code scanning on non-GitHub CI/CD systems and requires a GitHub access token to connect to a GitHub repository. The runner and its documentation previously suggested passing the GitHub token as a command-line parameter to the process instead of reading it from a file, standard input, or an environment variable. This approach made the token visible to other processes on the same machine, for example in the output of the `ps` command. If the CI system publicly exposes the output of `ps`, for example by logging the output, then the GitHub access token can be exposed beyond the scope intended. Users of the CodeQL runner on 3rd-party systems, who are passing a GitHub token via the `--github-auth` flag, are affected. This applies to both GitHub.com and GitHub Enterprise users. Users of the CodeQL Action on GitHub Actions are not affected. The `--github-auth` flag is now considered insecure and deprecated. The undocumented `--external-repository-token` flag has been removed. To securely provide a GitHub access token to the CodeQL runner, users should **do one of the following instead**: Use the `--github-auth-stdin` flag and pass the token on the command line via standard input OR set the `GITHUB_TOKEN` environment variable to contain the token, then call the command without passing in the token. The old flag remains present for backwards compatibility with existing workflows. If the user tries to specify an access token using the `--github-auth` flag, there is a deprecation warning printed to the terminal that directs the user to one of the above options. All CodeQL runner releases codeql-bundle-20210304 onwards contain the patches. We recommend updating to a recent version of the CodeQL runner, storing a token in your CI system's secret storage mechanism, and passing the token to the CodeQL runner using `--github-auth-stdin` or the `GITHUB_TOKEN` environment variable. If still using the old flag, ensure that process output, such as from `ps`, is not persisted in CI logs.

CVE-2021-32638 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **github** - **codeql-action** version **< codeql-bundle-20210304**

CVSS3 Score: 4.4 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
Remove --external-repository-token option from runner · github/codeql-action@58defc0 · GitHub	github.com text/html	MISC github.com/github/codeql-action/commit/58defc0652e935f6f2ffc70a82828b98d75476fb
Release CodeQL Bundle · github/codeql-action · GitHub	github.com text/html	MISC github.com/github/codeql-action/releases/tag/codeql-bundle-20210304
Passing Passwords	www.netmeister.org text/html	MISC www.netmeister.org/blog/passing-passwords.html
Add capability to specify auth from env var or stdin · github/codeql-action@88714e3 · GitHub	github.com text/html	MISC github.com/github/codeql-action/commit/88714e3a60e72ec53caa0e6a203652ee1f3fb1db
CodeQL runner: Command-line options that make GitHub access tokens visible to other processes are now deprecated · Advisory · github/codeql-action · GitHub	github.com text/html	CONFIRM github.com/github/codeql-action/security/advisories/GHSA-g36v-2xff-pv5m

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Github	Codeql Action	All	All	All	All

cpe:2.3:a:github:codeql_action:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32638 : Github's CodeQL action is provided to run CodeQL-based code scanning on non-GitHub CI/CD systems a… twitter.com/i/web/status/1…	2021-05-25 17:17:41
/r/netcve	CVE-2021-32638	2021-05-25 17:41:35

← Previous ID

Next ID→