CodeQL runner: Command-line options that make GitHub access tokens visible to other processes are now deprecated

Moderate **adityasharad** published **GHSA-g36v-2xff-pv5m** on May 25, 2021

Package

CodeQL runner (CodeQL runner)

Affected versions	Patched versions
< codeql-bundle-20210304	codeql-bundle-20210304

Description

Impact

The CodeQL runner tool, provided to run CodeQL-based code scanning on non-GitHub CI/CD systems, 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. For example:

```
/path/to-runner/codeql-runner-linux <command> <args> --github-auth TOKEN
```

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.

Mitigation / new behavior

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:

  ```
  echo "$TOKEN" | /path/to-runner/codeql-runner-linux <command> <args> --github-auth-stdin
  ```

- Set the `GITHUB_TOKEN` environment variable to contain the token, then call the command without passing in the token:

  ```
  # set GITHUB_TOKEN to the token, using your CI system's secret storage mechanism
  /path/to-runner/codeql-runner-linux <command> <args>
  ```

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.

For more information, see the GitHub documentation pages linked below.

Patches

All CodeQL runner releases from https://github.com/github/codeql-action/releases/tag/codeql-bundle-20210304 onwards contain the patches:

- `88714e3` deprecates the `--github-auth` flag
- `58defc0` removes the `--external-repository-token` flag

Workarounds

- 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.

References

- GitHub documentation
  - https://docs.github.com/en/code-security/secure-coding/using-codeql-code-scanning-with-your-existing-ci-system/running-codeql-runner-in-your-ci-system
  - https://docs.github.com/en/code-security/secure-coding/using-codeql-code-scanning-with-your-existing-ci-system/configuring-codeql-runner-in-your-ci-system#init
- https://cwe.mitre.org/data/definitions/214.html
- https://www.netmeister.org/blog/passing-passwords.html

For more information

If you have any questions or comments about this advisory:

- Open an issue
- Contact us as described in the security policy

Credit

Thanks to `@jlleitschuh` for reporting this vulnerability through our Bug Bounty program.

Severity

Moderate 4.4 / 10

CVSS base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	None
Availability	None

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVE ID

CVE-2021-32638

Weaknesses

CWE-214

Credits

 JLLeitschuh