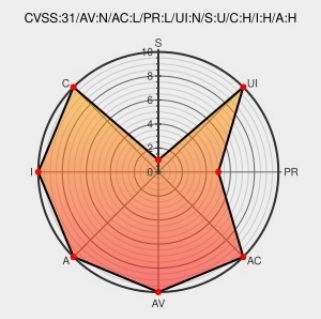
CVE-2023-27581

Published on: Not Yet Published

Last Modified on: 03/17/2023 04:05:00 PM UTC

CVE-2023-27581 - advisory for GHSA-6q4m-7476-932w

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



Certain versions of Github-slug-action from Github-slug-action Project contain the following vulnerability:

github-slug-action is a GitHub Action to expose slug value of GitHub environment variables inside of one's GitHub workflow. Starting in version 4.0.0` and prior to version 4.4.1, this action uses the `github.head_ref` parameter in an insecure way. This vulnerability can be triggered by any user on GitHub on any workflow using the action on pull requests. They just need to create a pull request with a branch name, which can contain the attack payload. This can be used to execute code on the GitHub runners and to exfiltrate any secrets one uses in the CI pipeline. A patched action is available in version 4.4.1. No workaround is available.

CVE-2023-27581 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **rlespinasse** - **github-slug-action** version **= >= 4.0.0, < 4.4.1**

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
github-slug-action vulnerable to arbitrary code execution · Advisory · rlespinasse/github-slug-action · GitHub	github.com text/html	MISC github.com/rlespinasse/github-slug-action/security/advisories/GHSA-6q4m-7476-932w
fix: use github.head_ref env var as trusted input · rlespinasse/github-slug-action@102b1a0 · GitHub	github.com text/html	MISC github.com/rlespinasse/github-slug-action/commit/102b1a064a9b145e56556e22b18b19c624538d94

Release v4.4.1 · rlespinasse/github-slug-action · GitHub	github.com text/html	MISC github.com/rlespinasse/github-slug-action/releases/tag/v4.4.1
Keeping your GitHub Actions and workflows secure Part 2: Untrusted input | GitHub Security Lab	securitylab.github.com text/html	MISC securitylab.github.com/research/github-actions-untrusted-input/

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	Github-slug-action Project	Github-slug-action	All	All	All	All

cpe:2.3:a:github-slug-action_project:github-slug-action:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-27581 : github-slug-action is a GitHub Action to expose slug value of GitHub environment variables inside… twitter.com/i/web/status/1…	2023-03-13 21:06:09
/r/netcve	CVE-2023-27581	2023-03-13 21:38:41

← Previous ID

Next ID→