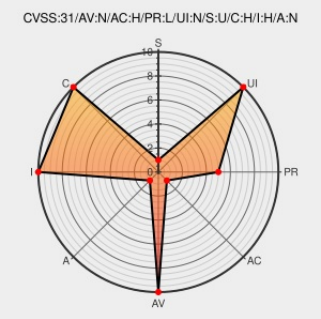
CVE-2021-21423

Published on: 04/06/2021 12:00:00 AM UTC

Last Modified on: 04/15/2021 02:37:00 PM UTC

CVE-2021-21423 - advisory for GHSA-gg2g-m5wc-vccq

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



Certain versions of Projen from Projen Project contain the following vulnerability:

`projen` is a project generation tool that synthesizes project configuration files such as `package.json`, `tsconfig.json`, `.gitignore`, GitHub Workflows, `eslint`, `jest`, and more, from a well-typed definition written in JavaScript. Users of projen's `NodeProject` project type (including any project type derived from it) include a `.github/workflows/rebuild-bot.yml` workflow that may allow any GitHub user to trigger execution of un-trusted code in the context of the "main" repository (as opposed to that of a fork). In some situations, such untrusted code may potentially be able to commit to the "main" repository. The rebuild-bot workflow is triggered by comments including `@projen rebuild` on pull-request to trigger a re-build of the projen project, and updating the pull request with the updated files. This workflow is triggered by an `issue_comment` event, and thus always executes with a `GITHUB_TOKEN` belonging to the repository into which the pull-request is made (this is in contrast with workflows triggered by `pull_request` events, which always execute with a `GITHUB_TOKEN` belonging to the repository from which the pull-request is made). Repositories that do not have branch protection configured on their default branch (typically `main` or `master`) could possibly allow an untrusted user to gain access to secrets configured on the repository (such as NPM tokens, etc). Branch protection prohibits this escalation, as the managed `GITHUB_TOKEN` would not be able to modify the contents of a protected branch and affected workflows must be defined on the default branch.

CVE-2021-21423 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **projen** - **projen** version **>= 0.6.0, < 0.16.41**

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE

Scope	Confidentiality	Integrity	Availability

	Impact	Impact	Impact
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
fix(node): security vulnerability in rebuild-bot (#602) · projen/projen@36030c6 · GitHub	github.com text/html	MISC github.com/projen/projen/commit/36030c6a4b1acd0054673322612e7c70e9446643
Rebuild-bot workflow may allow unauthorised repository modifications · Advisory · projen/projen · GitHub	github.com text/html	CONFIRM github.com/projen/projen/security/advisories/GHSA-gg2g-m5wc-vccq
projen - npm	www.npmjs.com text/html	MISC www.npmjs.com/package/projen

Related QID Numbers

982750 Nodejs (npm) Security Update for projen (GHSA-gg2g-m5wc-vccq)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Projen Project	Projen	All	All	All	All

cpe:2.3:a:projen_project:projen:*:*:*:*:*:node.js:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-21423 : `projen` is a project generation tool that synthesizes project configuration files such as `packag… twitter.com/i/web/status/1…	2021-04-06 18:41:47
/r/netcve	CVE-2021-21423	2021-04-06 19:20:15

← Previous ID

Next ID→