



# CVE-2021-32724

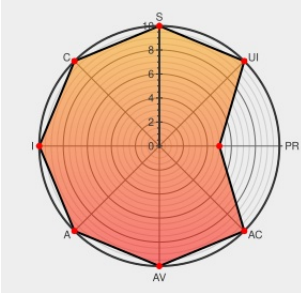
Published on: 09/09/2021 12:00:00 AM UTC

Last Modified on: 09/27/2021 02:21:00 PM UTC

## CVE-2021-32724 - advisory for GHSA-g86g-chm8-7r2p

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H



Certain versions of [Check-spelling](#) from [Check-spelling](#) contain the following vulnerability:

check-spelling is a github action which provides CI spell checking. In affected versions and for a repository with the [check-spelling action] (<https://github.com/marketplace/actions/check-spelling>) enabled that triggers on `pull\_request\_target` (or `schedule`), an attacker can send a crafted Pull Request that causes a `GITHUB\_TOKEN` to be

exposed. With the `GITHUB\_TOKEN`, it's possible to push commits to the repository bypassing standard approval processes. Commits to the repository could then steal any/all secrets available to the repository. As a workaround users may can either: [Disable the workflow](<https://docs.github.com/en/actions/managing-workflow-runs/disabling-and-enabling-a-workflow>) until you've fixed all branches or Set repository to [Allow specific actions] (<https://docs.github.com/en/github/administering-a-repository/managing-repository-settings/disabling-or-limiting-github-actions-for-a-repository#allowing-specific-actions-to-run>). check-spelling isn't a verified creator and it certainly won't be anytime soon. You could then explicitly add other actions that your repository uses. Set repository [Workflow permissions] ([https://docs.github.com/en/github/administering-a-repository/managing-repository-settings/disabling-or-limiting-github-actions-for-a-repository#setting-the-permissions-of-the-github\\_token-for-your-repository](https://docs.github.com/en/github/administering-a-repository/managing-repository-settings/disabling-or-limiting-github-actions-for-a-repository#setting-the-permissions-of-the-github_token-for-your-repository)) to `Read repository contents permission`. Workflows using `check-spelling/check-spelling@main` will get the fix automatically. Workflows using a pinned sha or tagged version will need to change the affected workflows for all repository branches to the latest version. Users can verify who and which Pull Requests have been running the action by looking up the spelling.yml action in the Actions tab of their repositories, e.g., <https://github.com/check-spelling/check-spelling/actions/workflows/spelling.yml> - you can filter PRs by adding `?query=event%3Apull\_request\_target`, e.g., [https://github.com/check-spelling/check-spelling/actions/workflows/spelling.yml?query=event%3Apull\\_request\\_target](https://github.com/check-spelling/check-spelling/actions/workflows/spelling.yml?query=event%3Apull_request_target).

CVE-2021-32724 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: check-spelling - check-spelling version < 0.0.19

CVSS3 Score: 9.9 - CRITICAL

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

CVSS2 Score: 6.8 - MEDIUM

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| NETWORK                | MEDIUM            | NONE                |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| PARTIAL                | PARTIAL           | PARTIAL             |

## CVE References

| Description                                                                                                                       | Tags                                                    | Link                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| check-spelling workflow vulnerable to GITHUB_TOKEN leakage via symlink attack · Advisory · check-spelling/check-spelling · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a> |  <a href="#">CONFIRM github.com/check-spelling/check-spelling/security/advisories/GHSA-g86g-chm8-7r2p</a>        |
| Merge pull request from GHSA-g86g-chm8-7r2p · check-spelling/check-spelling@436362f · GitHub                                      | <a href="#">github.com</a><br><a href="#">text/html</a> |  <a href="#">MISC github.com/check-spelling/check-spelling/commit/436362fc6b588d9d561cbdb575260ca593c8dc56</a> |

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](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

## Exploit/POC from Github

Dummy github repo for CVE-2021-32724 vulnerability exploit testing

### Known Affected Configurations (CPE V2.3)

| Type                                                              | Vendor                         | Product                        | Version | Update | Edition | Language |
|-------------------------------------------------------------------|--------------------------------|--------------------------------|---------|--------|---------|----------|
| Application                                                       | <a href="#">Check-spelling</a> | <a href="#">Check-spelling</a> | All     | All    | All     | All      |
| <code>cpe:2.3:a:check-spelling:check-spelling:*:*:*:*:*:*:</code> |                                |                                |         |        |         |          |

No vendor comments have been submitted for this CVE

## Social Mentions

| Source                                                                                         | Title                                                                                                                                                                                                    | Posted (UTC)             |
|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
|  @CVEreport    | CVE-2021-32724 : check-spelling is a github action which provides CI spell checking. In affected versions and for a... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2021-09-09 21:04:21      |
|  @JGamblin     | This was an interesting @github actions vulnerability (CVE-2021-32724): <a href="https://github.com/check-spelling...">github.com/check-spelling...</a>                                                  | 2021-09-09 21:57:07      |
|  /r/bag_o_news | <a href="#">CVE-2021-32724 - GitHub Actions check-spelling community workflow - GITHUB_TOKEN leakage via advice.txt symlink</a>                                                                          | 2021-09-10 10:05:48      |
| <a href="#">← Previous ID</a>                                                                  |                                                                                                                                                                                                          | <a href="#">Next ID→</a> |

© 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 registered 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](#)