

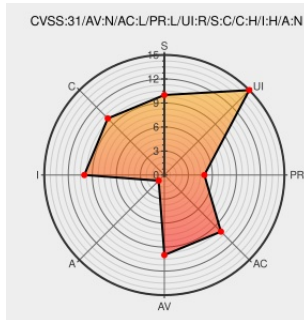


CVE-2020-15272

Published on: 10/26/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:42 PM UTC

CVE-2020-15272 - advisory for GHSA-hgx2-4pp9-357g

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

Certain versions of [Git-tag-annotation-action](#) from [Git-tag-annotation-action Project](#) contain the following vulnerability:

In the git-tag-annotation-action (open source GitHub Action) before version 1.0.1, an attacker can execute arbitrary (*) shell commands if they can control the value of [the `tag` input] or manage to alter the value of [the `GITHUB\_REF` environment variable]. The problem has been patched in version 1.0.1. If you don't use the `tag` input you are most likely safe. The `GITHUB\_REF` environment variable is protected by the GitHub Actions environment so attacks from there should be impossible. If you must use the `tag` input and cannot upgrade to `> 1.0.0` make sure that the value is not controlled by another Action.

CVE-2020-15272 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: ericcornelissen - git-tag-annotation-action version < 1.0.1

CVSS3 Score: **9.6 - CRITICAL**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Shell-injection through Action input · Advisory · ericcornelissen/git-tag-annotation-action · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/ericcornelissen/git-tag-annotation-action/security/advisories/GHSA-hgx2-4pp9-357g
Release Release v1.0.1 · ericcornelissen/git-tag-annotation-action · GitHub	Third Party Advisory github.com text/html	 MISC github.com/ericcornelissen/git-tag-annotation-action/releases/tag/v1.0.1
Fix shell injection bug · ericcornelissen/git-tag-annotation-action@9f30756 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/ericcornelissen/git-tag-annotation-action/commit/9f30756375cc4b1b6c66f274fc9c591fa901455a

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	Git-tag-annotation-action Project	Git-tag-annotation-action	All	All	All	All
Application	Git-tag-annotation-action Project	Git-tag-annotation-action	All	All	All	All

cpe:2.3:a:git-tag-annotation-action_project:git-tag-annotation-action:*.***.***.***:*

cpe:2.3:a:git-tag-annotation-action_project:git-tag-annotation-action:*.***.***.***:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →