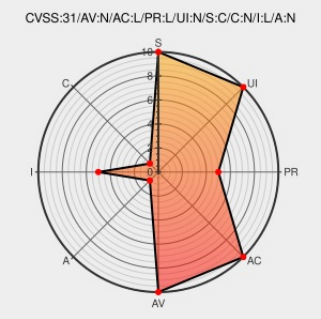
CVE-2022-35954

Published on: Not Yet Published

Last Modified on: 08/16/2022 04:54:00 PM UTC

CVE-2022-35954 - advisory for GHSA-7r3h-m5j6-3q42

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



Certain versions of Toolkit from Github contain the following vulnerability:

The GitHub Actions ToolKit provides a set of packages to make creating actions easier. The `core.exportVariable` function uses a well known delimiter that attackers can use to break out of that specific variable and assign values to other arbitrary variables. Workflows that write untrusted values to the `GITHUB_ENV` file may cause the path or other environment variables to be modified without the intention of the workflow or action author. Users should upgrade to `@actions/core v1.9.1`. If you are unable to upgrade the `@actions/core` package, you can modify your action to ensure that any user input does not contain the delimiter `_GitHubActionsFileCommandDelimeter_` before calling `core.exportVariable`.

CVE-2022-35954 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **actions** - **toolkit** version **<= 1.9.0**

CVSS3 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Delimiter injection vulnerability in @actions/core exportVariable · Advisory · actions/toolkit · GitHub	github.com text/html	CONFIRM github.com/actions/toolkit/security/advisories/GHSA-7r3h-m5j6-3q42

Merge pull request from GHSA-7r3h-m5j6-3q42 · actions/toolkit@4beda9c · GitHub	github.com text/html	MISC github.com/actions/toolkit/commit/4beda9cbc00ba6eefe387a937c21087ccb8ee9df

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Github	Toolkit	All	All	All	All

cpe:2.3:a:github:toolkit:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-35954 : The GitHub Actions ToolKit provides a set of packages to make creating actions easier. The `core.e… twitter.com/i/web/status/1…	2022-08-13 23:44:13
/r/netcve	CVE-2022-35954	2022-08-14 00:38:41

← Previous ID

Next ID→