



CVE-2023-23939

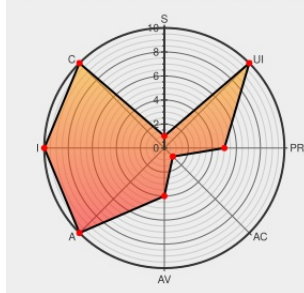
Published on: Not Yet Published

Last Modified on: 11/07/2023 04:08:00 AM UTC

CVE-2023-23939 - advisory for GHSA-p756-rfxh-x63h

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

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



Certain versions of [Azure Setup Kubectrl](#) from [Microsoft](#) contain the following vulnerability:

Azure/setup-kubectrl is a GitHub Action for installing Kubectrl. This vulnerability only impacts versions before version 3. An insecure temporary creation of a file allows other actors on the Actions runner to replace the Kubectrl binary created by this action because it is world writable. This Kubectrl tool installer runs ``fs.chmodSync(kubectrlPath,`

`777)`` to set permissions on the Kubectrl binary, however, this allows any local user to replace the Kubectrl binary. This allows privilege escalation to the user that can also run kubectrl, most likely root. This attack is only possible if an attacker somehow breached the GitHub actions runner or if a user is utilizing an Action that maliciously executes this attack. This has been fixed and released in all versions ``v3`` and later. 775 permissions are used instead. Users are advised to upgrade. There are no known workarounds for this issue.

CVE-2023-23939 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Azure](#) - [setup-kubectrl](#) version = `< 3`

CVSS3 Score: **7 - HIGH**

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

CVE References

Description	Tags	Link
lower permissions for chmod (#51) · Azure/setup-kubectrl@d449d75 · GitHub	github.com text/html	MISC github.com/Azure/setup-kubectrl/commit/d449d75495d2b9d1463555bb00ca3dca77a42ab6
Azure/setup-kubectrl: Escalation of privilege vulnerability	github.com	MISC github.com/Azure/setup-

Azure/setup-kubectrl: Escalation of privilege vulnerability for v3 and lower · Advisory · Azure/setup-kubectrl · GitHub

github.com

github.com/Azure/setup-kubectrl/security/advisories/GHSA-p756-rfxh-x63h

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	Microsoft	Azure Setup Kubectrl	All	All	All	All

cpe:2.3:a:microsoft:azure_setup_kubectrl:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-23939 : Azure/setup-kubectrl is a GitHub Action for installing Kubectrl. This vulnerability only impacts ver... twitter.com/i/web/status/1...	2023-03-06 19:02:44
/r/netcve	CVE-2023-23939	2023-03-06 20:38:05
/r/Team_IT_Security	CVE-2023-23939 Microsoft Azure setup-kubectrl prior 3 permission assignment (GHSA-p756-rfxh-x63h)	2023-03-31 21:37:10

← Previous ID

Next ID→