

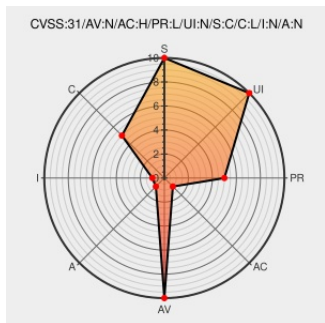


CVE-2020-15228

Published on: 10/01/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 05:52:00 PM UTC

CVE-2020-15228 - advisory for GHSA-mfwh-5m23-j46w

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

Certain versions of [Toolkit](#) from [Toolkit Project](#) contain the following vulnerability:

In the `@actions/core` npm module before version 1.2.6, `addPath` and `exportVariable` functions communicate with the Actions Runner over stdout by generating a string in a specific format. Workflows that log untrusted data to stdout may invoke these commands, resulting in the path or environment variables being modified without the intention of

the workflow or action author. The runner will release an update that disables the `set-env` and `add-path` workflow commands in the near future. For now, users should upgrade to `@actions/core v1.2.6` or later, and replace any instance of the `set-env` or `add-path` commands in their workflows with the new Environment File Syntax. Workflows and actions using the old commands or older versions of the toolkit will start to warn, then error out during workflow execution.

CVE-2020-15228 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: actions - toolkit version < 1.2.6

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality	Integrity	Availability

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

NONE

CVE References

Description

GitHub Widespread Injection ≈ Packet Storm

`add-path` and `set-env` Runner commands are processed via stdout · Advisory · actions/toolkit · GitHub

Tags

Exploit

Third Party Advisory

VDB Entry

packetstormsecurity.com

text/html

Third Party Advisory

github.com

text/html

Link

MISC

packetstormsecurity.com/files/159794/GitHub-Widespread-Injection.html

CONFIRM

github.com/actions/toolkit/security/advisories/GHSA-mfwh-5m23-j46w

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.

Related QID Numbers

980056 Nodejs (npm) Security Update for @actions/core (GHSA-mfwh-5m23-j46w)

Exploit/POC from Github

Fix CVE-2020-15228 (set-env, add-path in Github-Actions)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Toolkit Project	Toolkit	All	All	All	All
Application	Toolkit Project	Toolkit	All	All	All	All
cpe:2.3:a:toolkit_project:toolkit:*:*:*:*:node.js:*:*						
cpe:2.3:a:toolkit_project:toolkit:*:*:*:*:node.js:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @evntdrvn	@mountain_ghosts It did (set-env), until	2021-05-17 12:58:29
 @LinInfoSec	Npm - CVE-2020-15228: github.com/actions/toolki...	2021-11-18 21:46:12
 @setup_php	setup-php v1 is not vulnerable to CVE-2020-15228 and any issues claiming so are created in error (? with details)	2022-02-02 09:53:56

 /r/AZURE	CVE-2020-15228 redux: Azure DevOps Pipelines RCE	2021-04-01 12:56:12
 /r/azuredevops	CVE-2020-15228 redux: Azure DevOps Pipelines RCE	2021-04-01 12:51:56

[< Previous ID](#)
[Next ID >](#)

© [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](#)