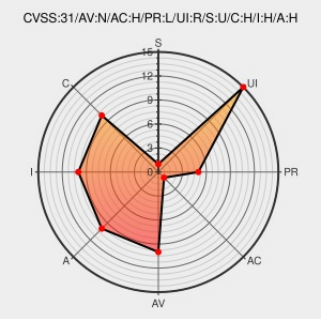
CVE-2022-29164

Published on: Not Yet Published

Last Modified on: 05/17/2022 01:49:00 PM UTC

CVE-2022-29164 - advisory for GHSA-cmv8-6362-r5w9

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



Certain versions of Argo Workflows from Argo Workflows Project contain the following vulnerability:

Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. In affected versions an attacker can create a workflow which produces a HTML artifact containing an HTML file that contains a script which uses XHR calls to interact with the Argo Server API. The attacker emails the deep-link to the artifact to their victim. The victim opens the link, the script starts running. As the script has access to the Argo Server API (as the victim), so may read information about the victim's workflows, or create and delete workflows. Note the attacker must be an insider: they must have access to the same cluster as the victim and must already be able to run their own workflows. The attacker must have an understanding of the victim's system. We have seen no evidence of this in the wild. We urge all users to upgrade to the fixed versions.

CVE-2022-29164 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **argoproj** - **argo-workflows** version **>= 2.6.0, < 3.2.11**

Affected Vendor/Software: **argoproj** - **argo-workflows** version **>= 3.3.0, < 3.3.5**

CVSS3 Score: 7.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Malicious HTML+XHR Artifact Privilege Escalation · Advisory · argoproj/argo-workflows · GitHub	github.com text/html	CONFIRM github.com/argoproj/argo-workflows/security/advisories/GHSA-cmv8-6362-r5w9
fix: Added artifact Content-Security-Policy (#8585) · argoproj/argo-workflows@87470e1 · GitHub	github.com text/html	MISC github.com/argoproj/argo-workflows/commit/87470e1c2bf703a9110e97bb755614ce8757fdcc
fix: Added artifact Content-Security-Policy by alexec · Pull Request #8585 · argoproj/argo-workflows · GitHub	github.com text/html	MISC github.com/argoproj/argo-workflows/pull/8585

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Argo Workflows Project	Argo Workflows	All	All	All	All

cpe:2.3:a:argo_workflows_project:argo_workflows:*:*:*:*:*:kubernetes:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29164 : Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs… twitter.com/i/web/status/1…	2022-05-05 23:21:34
@LinInfoSec	Kubernetes - CVE-2022-29164: github.com/argoproj/argo-…	2022-05-06 06:00:34
/r/netcve	CVE-2022-29164	2022-05-06 00:38:51

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report