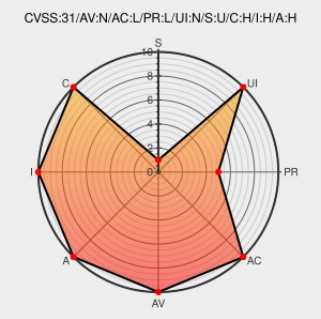
# CVE-2022-1025

Published on: Not Yet Published

Last Modified on: 06/27/2023 03:54:00 PM UTC

## CVE-2022-1025

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




Certain versions of Argo-cd from Linuxfoundation contain the following vulnerability:

All unpatched versions of Argo CD starting with v1.0.0 are vulnerable to an improper access control bug, allowing a malicious user to potentially escalate their privileges to admin-level.

CVE-2022-1025 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

### CVSS3 Score: 8.8 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | LOW | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 9 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | SINGLE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Red Hat Customer Portal - Access to 24x7 support and knowledge | access.redhat.com text/html | MISC access.redhat.com/errata/RHSA-2022:1040 |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | access.redhat.com | MISC |

| | | |
|---|---|---|
| | text/html | access.redhat.com/errata/RHSA-2022:1039 |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | access.redhat.com<br>text/html | MISC access.redhat.com/errata/RHSA-2022:1041 |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | access.redhat.com<br>text/html | MISC access.redhat.com/security/cve/CVE-2022-1025 |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | access.redhat.com<br>text/html | MISC access.redhat.com/errata/RHSA-2022:1042 |
| Improper access control allows admin privilege escalation · Advisory · argoproj/argo-cd · GitHub | github.com<br>text/html | MISC github.com/argoproj/argo-cd/security/advisories/GHSA-2f5v-8r3f-8pww |
| 2064682 – (CVE-2022-1025) CVE-2022-1025 Openshift-Gitops: Improper access control allows admin privilege escalation | bugzilla.redhat.com<br>text/html | MISC bugzilla.redhat.com/show_bug.cgi?id=2064682 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Linuxfoundation | Argo-cd | All | All | All | All |
| Application | Linuxfoundation | Argo-cd | All | All | All | All |
| Application | Linuxfoundation | Argo-cd | All | All | All | All |

cpe:2.3:a:linuxfoundation:argo-cd:*:*:*:*:*:*:*:*:

cpe:2.3:a:linuxfoundation:argo-cd:*:*:*:*:*:*:*:*:

cpe:2.3:a:linuxfoundation:argo-cd:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @antitree | ArgoCD CVE-2022-1025 looks pretty critical. Priv esc via a whole bunch of access levels. ? ? CVSS 9.9 if you belie… twitter.com/i/web/status/1… | 2022-03-23 19:39:51 |
| @AmitaiCo | @antitree NVD seems to list this vulnerability as CVE-2022-24768 (), whereas CVE-2022-1025 i… twitter.com/i/web/status/1… | 2022-03-24 07:54:53 |
| @ipssignatures | The vuln CVE-2022-1025 has a tweet created 0 days ago and retweeted 13 times. twitter.com/antitree/statu… #pow1rtrtwwcve | 2022-03-24 08:06:01 |

| | | |
|---|---|---|
| @eyenx | 2022 is a nightmare of a year CVE-2022-1025 #ArgoCD github.com/argoproj/argo-… | 2022-03-24 08:50:30 |
| @csantanapr | PSA: Time to patch your argocd today CVE-2022-1025 github.com/argoproj/argo-… argocd users make sure to update, high… twitter.com/i/web/status/1… | 2022-03-24 12:49:09 |
| @ericsmalling | @snyksec FYI - We've just updated this document to reflect newer upgrade versions in response to the recently announced CVE-2022-1025 | 2022-03-24 15:08:38 |
| @oldmanuk | @bboreham Nobody was accounting on CVE-2022-1025 shipping though | 2022-03-27 15:53:07 |
| @CVEreport | CVE-2022-1025 : All unpatched versions of Argo CD starting with v1.0.0 are vulnerable to an improper access control… twitter.com/i/web/status/1… | 2022-07-12 21:03:32 |

← Previous ID

Next ID→