# Improper access control allows admin privilege escalation

Critical **alexmt** published **GHSA-2f5v-8r3f-8pww** on Mar 23

Package

**github.com/argoproj/argo-cd** (Go)

Affected versions

0.5.0 through 2.1.12, 2.2.7, 2.3.1

Patched versions

2.3.2, 2.2.8, 2.1.14

## Description

### Impact

#### Impacts for versions starting with v1.0.0

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.

To perform the following exploits, an authorized Argo CD user must have push access to an Application's source git or Helm repository or `sync` *and* `override` access to an Application. Once a user has that access, different exploitation levels are possible depending on their other RBAC privileges:

1. If that user has `update` access to the Application, they can modify any resource on the Application's destination cluster. If the destination cluster is or can be made to be the same as the cluster hosting Argo CD, the user can escalate their Argo CD permissions to admin-level.
2. If the user has `delete` access to the Application, they can delete any resource on the Application's destination cluster. (This exploit is possible starting with v0.8.0.)
3. If the user has `get` access to the Application, they can view any resource on the Application's destination cluster (except for the contents of Secrets) and list actions available for that resource.
4. If the user has `get` access to the Application, they can view the logs of any Pods on the Application's destination cluster.
5. If the user has `action/{some action or *}` access on the Application, they can run an action for any resource (which supports the allowed action(s)) on the Application's destination cluster. (Some actions are available in Argo CD by default, and others may be configured by an Argo CD admin.)

See the Argo CD RBAC documentation for an explanation of the privileges available in Argo CD.

#### Events exploit

A related exploit is possible for a user with `get` access to an Application **even if they do not have access to the Application's source git or Helm repository or `sync` and `override` access to the Application**. The user can access any Event in the Application's destination cluster if they know the involved object's name, UID, and namespace.

#### Impacts for versions starting with v0.8.0

The same bug exists starting with v0.8.0, but only the following exploits were possible before v1.0.0:

- The `delete` exploit (#2 above).
- The logs exploit (#4 above).
- The Events exploit described above.

#### Impacts for versions starting with v0.5.0

The same bug exists starting with v0.5.0 (when RBAC was implemented), but only the Events exploit described above was possible before v0.8.0.

## Patches

A patch for this vulnerability has been released in the following Argo CD versions:

- v2.3.2
- v2.2.8
- v2.1.14

**Versions 2.0.x and earlier users:** See the changelog for links to upgrade instructions for your version. It is imperative to upgrade quickly, but some limited mitigations are described in the next section.

**argo-helm chart users:** Argo CD users deploying v2.3.x with argo-helm can upgrade the chart to version 4.2.2. Argo CD 2.2 and 2.1 users can set the `global.image.tag` value to the latest in your current release series ( `v2.2.8` , or `v2.1.14` ). Since charts for the 2.2 and 2.1 series are no longer maintained, you will need to either leave the value override in place or upgrade to the 4.x chart series (and therefore to Argo CD 2.3).

## Workarounds

The only certain way to avoid the vulnerability is to upgrade.

#### Mitigations

- To avoid privilege escalation:
  - Limit who has push access to Application source repositories or `sync + override` access to Applications.

    - Limit which repositories are available in projects where users have `update` access to Applications.
- To avoid unauthorized resource inspection/tampering:
    - Limit who has `delete`, `get`, or `action` access to Applications.

These mitigations can help limit potential damage, but they are *not* a substitute for upgrading. It is necessary to upgrade immediately.

## References

- Argo CD RBAC configuration documentation

## For more information

Open an issue in the Argo CD issue tracker or discussions
Join us on Slack in channel #argo-cd

**Severity**

Critical 9.9 / 10

| CVSS base metrics | |
|---|---|
| Attack vector | Network |
| Attack complexity | Low |
| Privileges required | Low |
| User interaction | None |
| Scope | Changed |
| Confidentiality | High |
| Integrity | High |
| Availability | High |

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

**CVE ID**

CVE-2022-1025

**Weaknesses**

CWE-200