



Argocd-image-updater: argocd image updater: cross-namespace privilege escalation via insufficient namespace validation

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-6388
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 22:17:22 UTC
Updated	2026-04-17 15:38:09 UTC
Description	A flaw was found in ArgoCD Image Updater. This vulnerability allows an attacker, with permissions to create or modify an Ir

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from secalert@redhat.com

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

EPSS: 0.000310000 probability, percentile 0.089040000 (date 2026-04-21)

Problem Types: CWE-1220 | CWE-1220 Insufficient Granularity of Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:L
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

High

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat OpenShift GitOps	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2026-6388	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2026-04-15T19:29:41.063Z	Reported to Red Hat.
CNA	2026-04-15T19:30:41.686Z	Made public.

Workarounds

CNA: Ensure that `AppProject` resources are configured to enforce strict tenant isolation within Red Hat OpenShift GitOps environments. Additionally, restrict the permissions of the Argo CD Image Updater controller to operate only within its designated namespaces, and limit the ability of users to create or modify `ImageUpdater` resources to trusted administrators. This reduces the risk of unauthorized cross-namespace application updates.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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