



# CVE-2020-11576

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-11576
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-08 18:15:00 UTC
<b>Updated</b>	2022-04-06 16:32:00 UTC
<b>Description</b>	Fixed in v1.5.1, Argo version v1.5.0 was vulnerable to a user-enumeration vulnerability which allowed attackers to determine

## Risk And Classification

**Problem Types:** CWE-203

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cncf	Argo Continuous Delivery	All	All	All	All
Application	Linuxfoundation	Argo Continuous Delivery	1.5.0	-	All	All

## References

Reference	Source	Link	Tags
Argo CVEs	MISC	<a href="http://www.soluble.ai">www.soluble.ai</a>	Threat
feat: implement Service Account / Local Users by alexmt · Pull Request #3215 · argoproj/argo-cd · GitHub	MISC	<a href="https://github.com">github.com</a>	Package
fix: return 401 error code if username does not exist (#3369) · argoproj/argo-cd@35a7350 · GitHub	MISC	<a href="https://github.com">github.com</a>	Package
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	Category
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	Category

No vendor comments have been submitted for this CVE.

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

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](#)**