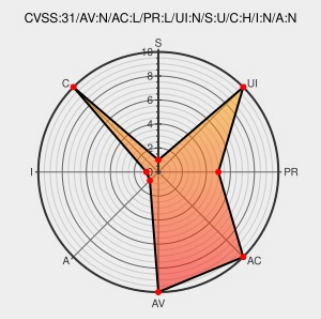
CVE-2023-42663

Published on: Not Yet Published

Last Modified on: 10/18/2023 06:46:00 PM UTC

CVE-2023-42663

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



Certain versions of Airflow from Apache contain the following vulnerability:

Apache Airflow, versions before 2.7.2, has a vulnerability that allows an authorized user who has access to read specific DAGs only, to read information about task instances in other DAGs. Users of Apache Airflow are advised to upgrade to version 2.7.2 or newer to mitigate the risk associated with this vulnerability.

CVE-2023-42663 has been assigned by security@apache.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache Airflow** version **< 2.7.2**

CVSS3 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/xj86cvfkxgd0cyqfmz6mh1bsfc61c6o9
REST API: Fix task instance access issue in the batch endpoint by ephraimbuddy · Pull Request #34315 · apache/airflow · GitHub	github.com text/html	MISC github.com/apache/airflow/pull/34315

Related QID Numbers

995608 Python (Pip) Security Update for apache-airflow (GHSA-32wr-qqw6-5mfp)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Airflow	All	All	All	All

cpe:2.3:a:apache:airflow:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→