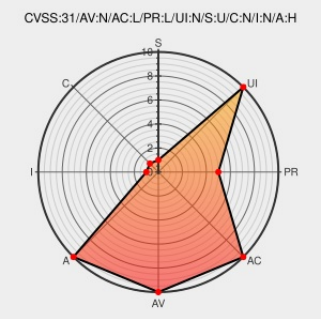
CVE-2023-22888

Published on: Not Yet Published

Last Modified on: 07/20/2023 03:42:00 PM UTC

CVE-2023-22888

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



Certain versions of Airflow from Apache contain the following vulnerability:

Apache Airflow, versions before 2.6.3, is affected by a vulnerability that allows an attacker to cause a service disruption by manipulating the run_id parameter. This vulnerability is considered low since it requires an authenticated user to exploit it. It is recommended to upgrade to a version that is not affected

CVE-2023-22888 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 **< 2.6.3**

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	NONE	NONE	HIGH

CVE References

Description	Tags	Link
Sanitize `DagRun.run_id` and allow flexibility by ephraimbuddy · Pull Request #32293 · apache/airflow · GitHub	github.com text/html	MISC github.com/apache/airflow/pull/32293
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/dnlht2hvm7k81k5tgjtsfmk27c76kq7z

There are currently no QIDs associated with this CVE

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

Social Mentions

Source	Title	Posted (UTC)
@oss_security	CVE-2023-22888: Apache Airflow: Scheduler remote DoS: Posted by Ephraim Anierobi on Jul 11Severity: low Affected… twitter.com/i/web/status/1…	2023-07-11 18:29:08
@CVEreport	CVE-2023-22888 : #Apache Airflow, versions before 2.6.3, is affected by a vulnerability that allows an attacker to… twitter.com/i/web/status/1…	2023-07-12 10:09:10

← Previous ID

Next ID→