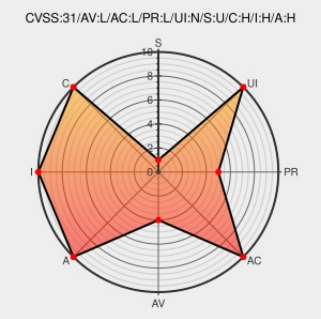
CVE-2022-38649

Published on: Not Yet Published

Last Modified on: 11/29/2022 01:47:00 PM UTC

CVE-2022-38649

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



Certain versions of Airflow from Apache contain the following vulnerability:

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Pinot Provider, Apache Airflow allows an attacker to control commands executed in the task execution context, without write access to DAG files. This issue affects Apache Airflow Pinot Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Apache Airflow Pinot Provider is installed (Apache Airflow Pinot Provider 4.0.0 can only be installed for Airflow 2.3.0+). Note that you need to manually install the Pinot Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version.

CVE-2022-38649 has been assigned by security@apache.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache Airflow Pinot Provider** version **< 4.0.0**

Affected Vendor/Software: **Apache Software Foundation** - **Apache Airflow** version **< 2.3.0**

CVSS3 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
The pinot-admin.sh command is now hard-coded. by potiuk · Pull Request #27641 · apache/airflow · GitHub	github.com text/html	MISC github.com/apache/airflow/pull/27641
No Description Provided	lists.apache.org	MISC

text/html	lists.apache.org/thread/033o1gbc4ly6dpd2xf1o201v56fbl4dz	

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
Application	Apache	Apache-airflow-providers-apache-pinot	All	All	All	All

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

cpe:2.3:a:apache:apache-airflow-providers-apache-pinot:*:*:*:*:*:*:*:*:

Discovery Credit

Apache Airflow PMC wants to thank id_No2015429 of 3H Security Team for reporting the issue.

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-38649	2022-11-22 10:38:24

← Previous ID

Next ID→