



CVE-2022-38170

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

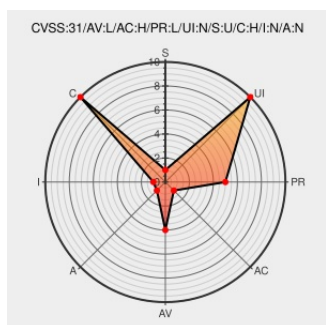
CVE-2022-38170

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Airflow](#) from [Apache](#) contain the following vulnerability:

In Apache Airflow prior to 2.3.4, an insecure umask was configured for numerous Airflow components when running with the `--daemon` flag which could result in a race condition giving world-writable files in the Airflow home directory and allowing local users to expose arbitrary file contents via the webserver.

CVE-2022-38170 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 **<= 2.3.3**

Vulnerability Patch/Work Around

Run without the `--daemon` flag via a process supervisor instead (systemd, runit, etc.).

CVSS3 Score: **4.7 - MEDIUM**

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

CVE References

Description	Tags	Link
oss-security - Re: CVE-2022-38170: Apache Airflow: Overly permissive umask for deamons	www.openwall.com text/html	MLIST [oss-security] 20220902 Re: CVE-2022-38170: Apache Airflow: Overly permissive umask for deamons
oss-security - CVE-2022-38170: Apache Airflow: Overly permissive umask for deamons	www.openwall.com text/html	MLIST [oss-security] 20220902 CVE-2022-38170: Apache Airflow: Overly permissive umask for deamons
oss-security - Re: CVE-2022-38170: Apache Airflow:	www.openwall.com	MLIST [oss-security] 20220920 Re: CVE-2022-38170:

Overly permissive umask for daemons

text/html

Apache Airflow: Overly permissive umask for daemons

No Description Provided

lists.apache.org

text/html

MISC

lists.apache.org/thread/zn8mbbb1j2od5nc9zhrvb7rpsrg1vvzv

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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:*:*:*:*:*:.

Discovery Credit

The Apache Airflow PMC would like to thank Harry Sintonen for reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-38170 : In #Apache Airflow prior to 2.3.4, an insecure umask was configured for numerous Airflow component... twitter.com/i/web/status/1...	2022-09-02 07:18:32
/r/netcve	CVE-2022-38170	2022-09-02 08:38:34

← Previous ID

Next ID→