



CVE-2023-40273

Published on: Not Yet Published

Last Modified on: 09/12/2023 07:10:21 AM UTC

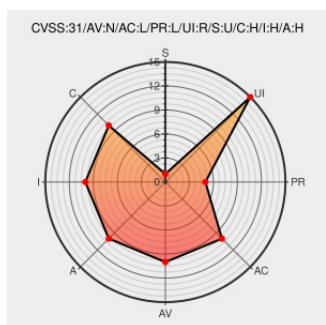
CVE-2023-40273

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The session fixation vulnerability allowed the authenticated user to continue accessing Airflow webserver even after the password of the user has been reset by the admin - up until the expiry of the session of the user. Other than manually cleaning the session database (for database session backend), or changing the secure_key and restarting

the webserver, there were no mechanisms to force-logout the user (and all other users with that). With this fix implemented, when using the database session backend, the existing sessions of the user are invalidated when the password of the user is reset. When using the securecookie session backend, the sessions are NOT invalidated and still require changing the secure key and restarting the webserver (and logging out all other users), but the user resetting the password is informed about it with a flash message warning displayed in the UI. Documentation is also updated explaining this behaviour. Users of Apache Airflow are advised to upgrade to version 2.7.0 or newer to mitigate the risk associated with this vulnerability.

CVE-2023-40273 has been assigned by security@apache.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache Airflow** version < 2.7.0

CVSS3 Score: **8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
-------------	------	------

No Description Provided

lists.apache.org

text/html

MISC

lists.apache.org/thread/9rdmv8ln4y4ncbyrlmjrsj903x4l80nj

oss-security - CVE-2023-40273: Session fixation in Apache Airflow web interface

www.openwall.com

text/html

MISC

www.openwall.com/lists/oss-security/2023/08/23/1

Remove user sessions when resetting password by potiuk · Pull Request #33347 · apache/airflow · GitHub

github.com

text/html

MISC

github.com/apache/airflow/pull/33347

oss-security - CVE-2023-40273: Session fixation in Apache Airflow web interface

www.openwall.com

text/html

MISC

www.openwall.com/lists/oss-security/2023/08/23/1

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:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →