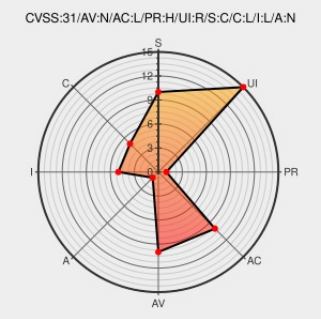
CVE-2019-12398

Published on: 01/14/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:03:00 AM UTC

CVE-2019-12398

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



Certain versions of Airflow from Apache contain the following vulnerability:

In Apache Airflow before 1.10.5 when running with the "classic" UI, a malicious admin user could edit the state of objects in the Airflow metadata database to execute arbitrary javascript on certain page views. The new "RBAC" UI is unaffected.

CVE-2019-12398 has been assigned by security@apache.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Apache** - **Airflow** version **Apache Airflow <= 1.10.4**

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Pony Mail!	Mailing List Vendor Advisory lists.apache.org	MLIST [airflow-dev] 20200114 [CVE-2019-12398] Apache Airflow Stored XSS vulnerability in classic UI

	text/html	
oss-security - [CVE-2019-12398] Apache Airflow Stored XSS vulnerability in classic UI	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20200114 [CVE-2019-12398] Apache Airflow Stored XSS vulnerability in classic UI
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	MLIST [airflow-users] 20200114 [CVE-2019-12398] Apache Airflow Stored XSS vulnerability in classic UI

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
Application	Apache	Airflow	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→