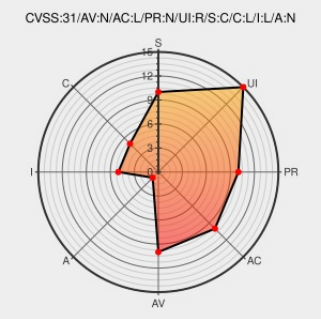
CVE-2020-17515

Published on: 12/11/2020 12:00:00 AM UTC

Last Modified on: 08/06/2022 03:50:00 AM UTC

CVE-2020-17515

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



Certain versions of Airflow from Apache contain the following vulnerability:

The "origin" parameter passed to some of the endpoints like '/trigger' was vulnerable to XSS exploit. This issue affects Apache Airflow versions prior to 1.10.13. This is same as CVE-2020-13944 but the implemented fix in Airflow 1.10.13 did not fix the issue completely.

CVE-2020-17515 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 **< 1.10.13**

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Pony Mail!	Issue Tracking, Mailing List, Vendor Advisory	MLIST [airflow-users] 20201211 CVE-2020-17515: Apache Airflow Reflected XSS via Origin Parameter

	lists.apache.org text/html	
Pony Mail!	lists.apache.org text/html	MLIST [announce] 20210501 Apache Airflow CVE: CVE-2021-28359: Apache Airflow Reflected XSS via Origin Query Argument in URL
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	MLIST [airflow-dev] 20201211 Apache Airflow Security Vulnerabilities fixed in v1.10.13: CVE-2020-17515
Pony Mail!	Issue Tracking Mailing List Vendor Advisory lists.apache.org text/html	MLIST [airflow-users] 20201211 Apache Airflow Security Vulnerabilities fixed in v1.10.13: CVE-2020-17515
oss-security - CVE-2021-28359: Apache Airflow Reflected XSS via Origin Query Argument in URL	www.openwall.com text/html	MLIST [oss-security] 20210501 CVE-2021-28359: Apache Airflow Reflected XSS via Origin Query Argument in URL
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	MLIST [announce] 20201211 Apache Airflow Security Vulnerabilities fixed in v1.10.13: CVE-2020-17515
Pony Mail!	lists.apache.org text/html	MLIST [airflow-users] 20210501 CVE-2021-28359: Apache Airflow Reflected XSS via Origin Query Argument in URL
oss-security - CVE-2020-17515: Apache Airflow Reflected XSS via Origin Parameter	Mailing List Vendor Advisory www.openwall.com text/html	MLIST [oss-security] 20201211 CVE-2020-17515: Apache Airflow Reflected XSS via Origin Parameter

Related QID Numbers

982683 Python (pip) Security Update for apache-airflow (GHSA-86vp-x3pr-79rx)

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

Discovery Credit

Ali Abdulwahab Ali Al-habsi of Accellion

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | The "origin" parameter passed to some of... | CVE-2020-17515 | Link for more: alerts.remotelyrmm.com/CVE-2020-17515	2022-08-06 05:29:23
@Har_sia	CVE-2020-17515 har-sia.info/CVE-2020-17515… #HarsiaInfo	2022-08-08 07:02:05

← Previous ID

Next ID→