

CVE-2020-13927

Apache Airflow's Experimental API Authentication Bypass

Exigent

CISA KEV since Jan 18, 2022

Actively exploited

Public exploit module (Metasploit)

The previous default setting for Airflow's Experimental API was to allow all API requests without authentication, but this poses security risks to users who miss this fact. From Airflow 1.10.11 the default has been changed to deny all requests by default and is documented at <https://airflow.apache.org/docs/1.10.11/security.html#api-authentication>.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.998 99.96th percentile · FIRST	CISA DEADLINE Jul 18, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.998 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Note this change fixes it for new installs but existing users need to change their config to default `[api]auth_backend = airflow.api.auth.backend.deny_all` as mentioned in the Updating Guide: <https://github.com/apache/airflow/blob/1.10.11/UPDATING.md#experimental-api-will-deny-all-request-by-default>

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
apache-airflow	< 1.10.11	1.10.11	GitHub
airflow	< 1.10.11	1.10.11	NVD

Sources

Vendor guidance github.com/advisories/GHSA-hhx9-p69v-cx2j

Additional guidance lists.apache.org/thread.html/r23a81b247aa346ff193670be565b2b8ea4b17ddbc7a35fc099c1aadd%40%3Cdev.airflow.apache.org%3Ecisa.gov/known-exploited-vulnerabilities-catalog

NVD nvd.nist.gov/vuln/detail/CVE-2020-13927

CISA KEV

ENISA EUVD europa.eu/enisa/eu-vulnerability/EUVD-2020-0037

Current data evulnabile.com/vulnerability-management/cve/CVE-2020-13927

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.