# CVE Detail – CVE-2020-13927

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. 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

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.99921

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-1056: Invokable Control Element with Variadic Parameters
* CWE-1188: Initialization of a Resource with an Insecure Default
* CWE-306: Missing Authentication for Critical Function

## CAPEC(s)

* CAPEC-12: Choosing Message Identifier
* CAPEC-166: Force the System to Reset Values
* CAPEC-216: Communication Channel Manipulation
* CAPEC-36: Using Unpublished Interfaces or Functionality
* CAPEC-62: Cross Site Request Forgery
* CAPEC-665: Exploitation of Thunderbolt Protection Flaws

## ATT&CK Techniques

* T1542.002: Component Firmware
* T1556: Modify Authentication Process
* T1211: Exploitation for Defense Evasion

## Used By (Actors/Tools)

* Cyclops Blink (malware)
* Kessel (malware)
* Ebury (malware)
* SILENTTRINITY (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Equation (intrusion-set)
* APT28 (intrusion-set)
* FIN13 (intrusion-set)

## Affected Products

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