**Overall Rating - Critical**

BRITISH COLUMBIA

**This notification is intended as an informational bulletin for technical audiences.**

## Summary

The Vulnerability and Risk Management (VRM) Team is aware 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.

## Technical Details

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

This vulnerability is rated as a **Critical** Severity.

## Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify VRM with any questions or concerns you may have.

## References

- CVE-2020-13927
- http://packetstormsecurity.com/files/162908/Apache-Airflow-1.10.10-Remote-Code-Execution.html
- http://packetstormsecurity.com/files/174764/Apache-Airflow-1.10.10-Remote-Code-Execution.html
- https://lists.apache.org/thread.html/r23a81b247aa346ff193670be565b2b8ea4b17ddbc7a35fc099c1aadd%40%3Cdev.airflow.apache.org%3E