مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Apache Airflow

Tracking #:432316579

Date:29-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in Apache Airflow, a widely-used workflow management platform. This vulnerability could potentially expose sensitive configuration data, including API keys, database credentials, and other critical secrets, within task logs.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-45784**
- CVSS Score: 7.5 (High)
- A vulnerability in Apache Airflow exposes sensitive configuration data in task logs, potentially compromising system security.
- The vulnerability stems from Airflow's failure to mask sensitive configuration values in task logs by default. This allows Directed Acyclic Graph (DAG) authors to unintentionally or intentionally log sensitive information such as API keys, database credentials, or other critical secrets.
- Successful exploitation of this vulnerability can lead to:
    - **Data breaches**: Exposure of confidential information, including API keys and database credentials
    - **System compromise**: Unauthorized access to critical systems using exposed credentials
    - **Lateral movement**: Potential for attackers to access other parts of the network

Affected Versions:

- Apache Airflow versions prior to 2.10.3

Fixed Versions:

- Apache Airflow version 2.10.3 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-45784