مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Security Updates – Apache Superset

Tracking #:432316103

Date:31-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apache released security updates to address a vulnerability in Apache Superset.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-34693** | Base Score: 6.8 - Medium | Improper Input Validation
  - Improper Input Validation vulnerability in Apache Superset, allows for an authenticated attacker to create a MariaDB connection with local_infile enabled.
  - If both the MariaDB server (off by default) and the local mysql client on the web server are set to allow for local infile, it's possible for the attacker to execute a specific MySQL/MariaDB SQL command that is able to read files from the server and insert their content on a MariaDB database table.
  - **Detailed proof of concept (PoC) and insights into potential impacts and exploitation methods is published.**

Affected Versions:

- Apache Superset before 3.1.3
- Apache Superset 4.0.0 before 4.0.1

Fixed Versions:

- Version 4.0.1 or 3.1.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Apache.

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://lists.apache.org/thread/1803x1s34m7r71h1k0q1njol8k6fmyon