مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Apache Superset

Tracking #:432317337

Date:02-06-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Apache Superset, a widely used open-source data visualization and business intelligence (BI) platform. The flaw allows authenticated attackers to bypass row-level security (RLS) controls using a SQL injection technique, potentially leading to unauthorized access to sensitive data.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-48912**
- CVSS Score 7.1 HIGH
- An authenticated user can exploit the sqlExpression field in Superset's RLS policies to inject arbitrary SQL subqueries. This allows them to evade fine-grained access restrictions configured via RLS, exposing data from datasets they would not normally be authorized to access.
- The vulnerability arises from insufficient sanitization of SQL expressions used in RLS configurations. specially crafted requests can bypass parser-level protections and inject malicious SQL payloads.
- **Affected Versions:** Apache Superset (All versions prior to 4.1.2)
- **Fixed Version:** 4.1.2 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache Superset.

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-2025-48912