مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in Apache Flink

Tracking #:432318981

Date:18-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Apache Flink could allow authenticated attackers to execute arbitrary code through specially crafted SQL queries due to improper input sanitization in SQL code generation.

TECHNICAL DETAILS:

A critical vulnerability in Apache Flink could allow authenticated users with query submission privileges to execute arbitrary code on TaskManagers through specially crafted SQL queries. The flaw is caused by improper input sanitization in SQL code generation, impacting vulnerable JSON functions and LIKE expressions with ESCAPE clauses. Successful exploitation may lead to system compromise, data manipulation, or service disruption.

Vulnerability Details

- **CVE-2026-35194 | Severity: Critical**
- Apache Flink contains a code injection flaw in its SQL code generation process that allows authenticated attackers to execute arbitrary code on TaskManagers via malicious SQL queries. The issue stems from improper escaping of user-controlled input during Java code generation.

Affected Versions

- Apache Flink 1.15.0 before 1.20.4,2.0.2,2.1.2,2.2.1

Fixed Versions:

- Apache Flink 1.20.4, 2.0.2, 2.1.2 or 2.2.1

RECOMMENDATIONS:

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

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/qh52bw4hhvy7n2owd8b3bt51mz0lvj9x