مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Improper Authentication Vulnerability in Apache Doris

Tracking #:432319317

Date:21-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability, CVE-2026-58319, has been identified in Apache Doris, a high-performance real-time analytical database.

TECHNICAL DETAILS:

A critical security vulnerability, CVE-2026-58319, has been identified in Apache Doris, a high-performance real-time analytical database. The vulnerability is caused by improper authentication in the Frontend (FE) HTTP REST administrative API, allowing certain administrative endpoints to be accessed without authentication.

An unauthenticated remote attacker with network access to the Frontend HTTP service could perform unauthorized administrative operations, potentially impacting cluster integrity, stability, and service availability. Successful exploitation could lead to disruption of database operations or denial-of-service (DoS) conditions.

Vulnerability Details:

- CVE-2026-58319 – Improper Authentication in Apache Doris Frontend HTTP API
- CVSS v3.1: 9.1 (Critical)
- The vulnerability is caused by improper authentication checks in the Apache Doris Frontend (FE) HTTP REST administrative API.
- Certain administrative HTTP REST endpoints can be accessed without requiring valid authentication credentials.
- A remote attacker with network connectivity to the FE HTTP service can send unauthorized administrative requests.
- No authentication or user interaction is required to exploit the vulnerability.
- The vulnerability may lead to denial-of-service (DoS) conditions or other operational disruptions.
- Apache Doris versions 2.1.0 through versions prior to 3.1.0 are affected.
- The issue has been resolved in Apache Doris version 3.1.0.

RECOMMENDATIONS:

Immediate Actions:

- Update Apache Doris to fixed version or later.

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://www.openwall.com/lists/oss-security/2026/07/14/3