مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Apache Parquet

Tracking #:432317045

Date:07-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical Remote Code Execution (RCE) vulnerability in Apache Parquet, which could potentially be exploited to gain complete control over the target system.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2025-30065
- CVSS v4: 10.0 (Critical)
- A critical remote code execution (RCE) vulnerability exists in Apache Parquet, a widely used open-source columnar data storage format. This flaw allows attackers to achieve arbitrary code execution by tricking users into importing maliciously crafted Parquet files.
- The vulnerability arises from unsafe deserialization during schema parsing in the parquet-avro module. It poses a severe risk to any big data pipeline, ETL tools, and analytics environments processing external or untrusted Parquet files.
- Successful exploitation can allow threat actors to:
    - Execute arbitrary code on the target system
    - Exfiltrate, alter, or destroy data
    - Deploy ransomware or other malicious payloads
    - Disrupt critical data services

Affected Versions:

- All versions up to and including 1.15.0

Fixed Version:

- Apache Parquet 1.15.1 or later

RECOMMENDATIONS:

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

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-2025-30065