مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in Apache Parquet

Tracking #:432317221

Date:07-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical vulnerability (CVE-2025-46762) has been discovered in the Apache Parquet Java library that allows Remote Code Execution (RCE).

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-46762) has been discovered in the Apache Parquet Java library, specifically affecting the parquet-avro module up to and including version 1.15.1. This flaw allows Remote Code Execution (RCE) when malicious Avro schemas embedded in Parquet file metadata are processed using unsafe deserialization models.
The vulnerability poses a significant threat to environments that leverage Apache Parquet in conjunction with the "specific" or "reflect" Avro deserialization models, especially when processing untrusted or user-supplied Parquet files. If exploited, attackers could execute arbitrary code on the affected system with the privileges of the application processing the file.

Vulnerability Details

- **CVE ID:** CVE-2025-46762
- **Severity:** Critical
- **Affected Component:** Apache Parquet Java – parquet-avro module
- **Affected Versions:** ≤ 1.15.1
- **Fixed Version:** 1.15.2 or for users on 1.15.1, Set the system property to an empty string "org.apache.parquet.avro.SERIALIZABLE_PACKAGES"
- **Impact:** Remote Code Execution (RCE)
- **Vector:** Malicious Avro schemas embedded in Parquet metadata
- **Conditions Required for Exploitation:**
  - Use of the parquet-avro module
  - Use of "specific" or "reflect" Avro deserialization models
  - Processing of untrusted or user-supplied Parquet files

RECOMMENDATIONS:

- Upgrade Apache Parquet Java to fixed versions.

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://seclists.org/oss-sec/2025/q2/103