AL2025_25 Critical RCE Vulnerability Discovered in Apache Parquet (CVE-2025-30065) (April 4th, 2025)

Description

A critical remote code execution (RCE) vulnerability (CVE-2025-30065) has been discovered in Apache Parquet, a widely used columnar storage format for big data and analytics applications. The vulnerability affects all versions up to and including 1.15.0 and carries the maximum CVSS v4 severity score of 10.0. This flaw, responsibly disclosed by Amazon researcher Keyi Li, was addressed in Apache Parquet version 1.15.1. It poses a severe threat to any system that processes Parquet files, especially those importing files from external or untrusted sources.

Attack Details

The vulnerability stems from unsafe deserialization in the parquet-avro module, which parses Parquet file schemas. An attacker can exploit this flaw by crafting a malicious Parquet file that, when ingested by a vulnerable system, results in arbitrary code execution. To exploit this vulnerability, the attacker must convince someone to import a specially crafted Parquet file into a vulnerable system.

This opens up a wide range of attack possibilities, including:

- System takeover
- Data theft or tampering
- Disruption of analytics services
- Deployment of ransomware or other malware

Apache Parquet is embedded in many enterprises' big data environments and platforms including Hadoop, Amazon Web Services (AWS), Google Cloud, Microsoft Azure, Netflix, Uber, Airbnb, LinkedIn, and others. Any environment processing external Parquet files is potentially at risk.

Remediation

Immediate action is advised for all organizations handling Parquet files:

- **Upgrade to Apache Parquet version 1.15.1**, which contains the patch for CVE-2025-30065.
- If an immediate upgrade is not feasible:
  - **Avoid importing Parquet files from untrusted or unknown sources.**
  - **Implement rigorous file validation** and sandbox testing before processing.
- **Increase monitoring and logging** on data ingestion systems to detect suspicious behavior.
- **Coordinate with development and vendor teams** to identify where vulnerable versions of Apache Parquet may be in use.
- Review data pipelines and **apply least privilege principles**, ensuring Parquet processing services operate with minimal permissions.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News. (n.d.). Critical flaw in Apache Parquet allows remote attackers to execute arbitrary code. Retrieved from The Hacker News. https://thehackernews.com/2025/04/critical-flaw-in-apache-parquet-allows.html
- Toulas, B. (2025, April 3). Max severity RCE flaw discovered in widely used Apache Parquet. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/max-severity-rce-flaw-discovered-in-widely-used-apache-parquet/