مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Apache Avro Java SDK

Tracking #:432316364

Date:04-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical security vulnerability, identified as CVE-2024-47561, has been discovered in the Apache Avro Java SDK.

TECHNICAL DETAILS:

A critical security vulnerability, identified as CVE-2024-47561, has been discovered in the Apache Avro Java SDK. This flaw affects all versions prior to 1.11.4 and allows attackers to execute arbitrary code on affected systems through maliciously crafted Avro data. Given the widespread use of Apache Avro in data serialization for various applications, organizations must act swiftly to mitigate potential risks associated with this vulnerability.

- **Vulnerability ID**: **CVE-2024-47561**
- The vulnerability arises from a flaw in the schema parsing functionality of the Java SDK. When a vulnerable system processes malicious Avro data, it can trigger the execution of arbitrary code, putting sensitive information and system integrity at risk.
- **Affected Versions**: All versions of Apache Avro Java SDK prior to 1.11.4
- **Impact**: Attackers can exploit this vulnerability to execute arbitrary code, potentially leading to:
    - Complete system compromise
    - Data breaches
    - Denial-of-service attacks
- **Fixed Versions**: Apache Avro Java SDK version 1.11.4 or 1.12.0

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the 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://lists.apache.org/thread/c2v7mhqnmq0jmbwxqq3r5jbj1xg43h5x