مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Apache Hive and Apache Spark

Tracking #:432316667

Date:25-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in Apache Hive and Apache Spark, widely used platforms for large-scale data processing and analytics. This vulnerability could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-23945**
- A security vulnerability has been identified in the CookieSigner mechanism of Apache Hive and Apache Spark. This flaw exposes valid cookie signatures when message verification fails, potentially allowing attackers to forge valid cookies and bypass security measures
- Successful exploitation of this vulnerability could lead to:
    - Unauthorized access to sensitive data
    - Bypass of authentication mechanisms
    - Potential for further system exploitation
- **Vulnerable Components:**
    - org.apache.hive:hive-service
    - org.apache.spark:spark-hive-thriftserver_2.11
    - org.apache.spark:spark-hive-thriftserver_2.12

Affected Versions:

- Apache Hive 1.2.0 before 4.0.0
- Apache Spark 2.0.0 before 3.0.0
- Apache Spark 3.0.0 before 3.3.4
- Apache Spark 3.4.0 before 3.4.2
- Apache Spark 3.5.0

Mitigation:

- update systems to the latest patched versions

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-2024-23945