مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Authentication Bypass Vulnerability in Apache HugeGraph-Server

Tracking #:432316677

Date:27-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical authentication bypass vulnerability has been discovered in Apache HugeGraph-Server, a widely used open-source graph database.

TECHNICAL DETAILS:

CVE-2024-43441 is a critical authentication bypass vulnerability found in Apache HugeGraph-Server, a widely used open-source graph database. This vulnerability, disclosed by the Apache Software Foundation on December 25, 2024, is rated as "important" and could allow attackers to bypass authentication mechanisms, leading to unauthorized access to sensitive graph data and operations. The flaw arises from improper handling of JWT tokens (JSON Web Tokens), specifically the assumption that certain JWT data is immutable, which can be exploited to manipulate the authentication process.

- Vulnerability ID: **CVE-2024-43441**
- Severity: Important
- Affected Product: Apache HugeGraph-Server
- Versions Affected: 1.0 to 1.3
- Exploit Type: Authentication Bypass
- Exploitable via: JWT token manipulation

Fixed Versions:

- Users of affected HugeGraph-Server versions (1.0–1.3) are strongly urged to upgrade to version 1.5.0

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://lists.apache.org/thread/h2607yv32wgcrywov960jpxhvsmmlf12