مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical SQL Injection Vulnerability in Apache Traffic Control

Tracking #:432316668
Date:25-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Apache Traffic Control, a widely-used open-source platform for building large-scale content delivery networks (CDNs). This vulnerability could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-45387**
- CVSS Score 9.9 (Critical)
- An SQL injection vulnerability exits in Traffic Ops in Apache Traffic Control. This vulnerability allows privileged users with specific roles (admin, federation, operations, portal, or steering) to execute arbitrary SQL commands against the database by sending a specially crafted PUT request to Traffic Ops. This could lead to severe consequences, including data manipulation, unauthorized access, and potential system compromise.

Affected Versions:

- Apache Traffic Control 8.0.0 through 8.0.1

Fixed Versions:

- Apache Traffic Control version 8.0.2 or later

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-2024-45387