مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

RCE Vulnerability in ThreatQuotient ThreatQ Platform

Tracking #:432316650

Date:19-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high Severity command injection vulnerability has been discovered in ThreatQuotient's ThreatQ Platform that could allow an attacker to perform remote code execution.

TECHNICAL DETAILS:

A high Severity command injection vulnerability (CVE-2024-39703) has been discovered in ThreatQuotient's ThreatQ Platform that allows remote attackers to execute arbitrary commands on the server, potentially leading to complete system compromise.

Vulnerability Details:

- CVE ID:**CVE-2024-39703**
- CVSS v3 Score: **8.8** (High)
- The vulnerability exists within the API endpoint of the ThreatQ Platform, where improper handling of user-supplied input can lead to the execution of arbitrary commands.

Affected Versions:

- ThreatQ Platform (versions prior to 5.29.3)

Fixed Versions:

- ThreatQ Platform: Version 5.29.3

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://www.cve.org/CVERecord?id=CVE-2024-39703