مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in QNAP Products

Tracking #:432315798

Date:29-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in QNAP products that could be exploited to gain unauthorized access on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-32766(CVSS10.0)-** An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network.

- **CVE-2024-32764(CVSS9.9)**- A missing authentication for critical function vulnerability has been reported to affect myQNAPcloud Link. If exploited, the vulnerability could allow users with the privilege level of some functionality via a network.

Affected Products:

- myQNAPcloud Link 2.4.x

Fixed Versions:

- myQNAPcloud Link 2.4.51 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by QNAP.

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.qnap.com/en-me/security-advisory/qsa-24-09