مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Zero-Day Vulnerability in QNAP QuRouter

Tracking #:432316476

Date:06-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical zero-day vulnerability has been discovered in the QNAP QuRouter network security appliance.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE ID: **CVE-2024-50389**
- Severity: (Critical)
- Affected Versions: QuRouter 2.4.x
- Fixed Version: QuRouter 2.4.5.032 and later

RECOMMENDATIONS:

- All users of QNAP QuRouter devices should update to fixed version as soon as possible.
- Monitor Systems: Conduct a thorough review of system logs and network traffic for any signs of unauthorized access or suspicious activity.
- Network Segmentation: Implement or review network segmentation to limit potential impact if a device is compromised.
- Access Controls: Strengthen access controls and authentication mechanisms for all network devices, especially those exposed to the internet.

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-24-45