مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Zero-day Vulnerability-QNAP NAS

Tracking #:432315878

Date:22-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that QNAP released emergency security updates to address multiple vulnerabilities in the QTS and QuTS hero.

TECHNICAL DETAILS:

QNAP released an emergency update for zero-day RCE vulnerability **CVE-2024-27130** and four more flaws in QNAP NAS products. The vulnerability details and a proof-of-concept (PoC) exploit have been publicly disclosed, increasing the risk of exploitation by malicious actors. If exploited, the vulnerability could allow users to execute code via a network.

Vulnerabilities addressed:

- CVE-2024-21902: If exploited, this vulnerability about incorrect permission assignment for critical resource could allow authenticated users to read or modify the resource via a network.
- CVE-2024-27127: If exploited, this double free vulnerability could allow authenticated users to execute arbitrary code via a network.
- CVE-2024-27128, CVE-2024-27129, CVE-2024-27130: If exploited, these vulnerabilities about buffer copy without checking size of input could allow authenticated users to execute arbitrary code via a network.

- **Affected Products:**
  - QTS 5.1.x & QuTS hero h5.1.x

- **Fixed Version:**
  - QTS 5.1.7.2770 build 20240520 and later
  - QuTS hero h5.1.7.2770 build 20240520 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the security patch as soon as possible.

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/security-advisory/qsa-24-23