CERT-EU

Security Advisory 2024-049

Multiple Vulnerabilities in QNAP Products

May 22, 2024 — v1.0

TLP:CLEAR

History:

- *22/05/2024 — v1.0 – Initial publication*

Summary

On May 21, 2024, QNAP released a security advisory addressing multiple flaws, including a zero-day vulnerability in the shared feature of QTS [1,2,3]. These vulnerabilities could allow remote attackers to execute arbitrary code.

It is strongly advised updating affected systems to the latest versions to mitigate these risks.

Technical Details

The vulnerability **CVE-2024-27130**, with a CVSS score of 7.2, is due to improper input validation in the shared feature of QTS that could allow remote attackers to execute arbitrary code. An attacker can exploit the vulnerability through a specially crafted request that causes a buffer overflow, leading to remote code execution. Successful exploitation requires access to a specific parameter [1,2].

Affected Products

- QTS QTS 5.1.x (fixed version is QTS 5.1.7.2770 build 20240520 and later) [3];
- QuTS hero h5.1.x (fixed version is QuTS hero h5.1.7.2770 build 20240520 and later) [3].

Recommendations

It is strongly recommended updating affected devices to a fixed version.

References

[1] https://www.bleepingcomputer.com/news/security/qnap-qts-zero-day-in-share-feature-gets-public-rce-exploit/

[2] https://labs.watchtowr.com/qnap-qts-qnapping-at-the-wheel-cve-2024-27130-and-friends/

[3] https://www.qnap.com/en/security-advisory/qsa-24-23