CERT-EU

Security Advisory 2023-087

Critical Vulnerabilities in QNAP products

November 7, 2023 — v1.0

TLP:CLEAR

History:

- *07/11/2023 — v1.0 – Initial publication*

Summary

On November 4 2023, QNAP Systems has released advisories [1,2] addressing critical vulnerabilities affecting multiple versions of the QTS operating system and applications on its network-attached storage (NAS) devices. These vulnerabilities could allow an attacker to achieve Remote Code Execution.

It is recommended updating affected devices as soon as possible.

Technical Details

- The vulnerability identified by `CVE-2023-23368`, with a CVSS score of 9.8 out of 10, is an OS command injection vulnerability. If exploited, the vulnerability could allow remote attackers to execute commands via a network.
- The vulnerability identified by `CVE-2023-23369`, with a CVSS score of 9.0 out of 10, is an OS command injection vulnerability. If exploited, the vulnerability could allow remote attackers to execute commands via a network.

Affected Products

- The vulnerability `CVE-2023-23368` affects the following products: QTS 5.0.x, QTS 4.5.x, QuTS hero h5.0.x, QuTS hero h4.5.x, and QuTScloud c5.0.x.
- The vulnerability `CVE-2023-23369` affects the following products: QTS 5.1.x, QTS 4.3.6, QTS 4.3.4, QTS 4.3.3, QTS 4.2.x, Multimedia Console 2.1.x, Multimedia Console 1.4.x, Media Streaming add-on 500.1.x, and Media Streaming add-on 500.0.x.

Recommendations

CERT-EU recommends to install updates as available following the QNAP procuct support status [3].

References

[1] https://www.qnap.com/en-uk/security-advisory/qsa-23-31

[2] https://www.qnap.com/en-uk/security-advisory/qsa-23-35

[3] https://www.qnap.com/en/product/status