CERT-EU

Security Advisory 2023-005

Critical Code Injection Vulnerability in QNAP Devices

January 31, 2023 — v1.0

TLP:CLEAR

History:

- *31/01/2023 — v1.0 – Initial publication*

Summary

On January 30th, 2023, QNAP published an advisory [1] related to a critical vulnerability, identified as `CVE-2022-27596`, allowing remote attackers to inject malicious code on QNAP NAS devices.

Technical Details

The vulnerability `CVE-2022-27596`, with a CVSS score of 9.8 out of 10, is due to a SQL injection flaw that allows attackers to send specially crafted requests on vulnerable devices in order to trigger unexpected behaviours, and especially malicious code execution.

Affected Products

The vulnerability affects the following QNAP operating system versions:

- QTS 5.0.1
- QuTS hero h5.0.1

Recommendations

CERT-EU recommends to follow the update procedure published by the QNAP team in its advisory [1].

References

[1] https://www.qnap.com/en/security-advisory/qsa-23-01