10 years CERT-EU

Security Advisory 2022-046

Critical PHP Flaw Exposes QNAP NAS Devices to RCE Attacks

June 22, 2022 — v1.0

TLP:WHITE

History:

- *22/06/2022 — v1.0 – Initial publication*

Summary

On 22nd of June 2022, QNAP published an advisory [1] about specific products that are vulnerable to remote code execution (RCE) when certain conditions are met. The CVE-2019-11043 is reported to affect PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11. In certain configurations of FPM setup, it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.

Technical Details

Certain QNAP NAS are vulnerable to RCE when the user has installed and is running `nginx` and `php-fpm`. QTS, QuTS hero or QuTScloud does not have `nginx` installed by default, thus QNAP NAS are not affected by this vulnerability in the default state. If `nginx` is installed by the user and running, then the update should be applied as soon as possible to mitigate associated risks.

Affected Products

The vulnerability affects the following QNAP operating system versions:

- QTS 5.0.x and later
- QTS 4.5.x and later
- QuTS hero h5.0.x and later
- QuTS hero h4.5.x and later
- QuTScloud c5.0.x and later

Recommendations

QNAP provided advice [2] for available updates and information on how to update the affected products.

References

[1] https://www.qnap.com/en/security-advisory/QSA-22-20

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