10 years CERT-EU

Security Advisory 2024-115

QNAP NAS Zero-Day Vulnerabilities

October 31, 2024 — v1.0

TLP:CLEAR

History:

- *31/10/2024 — v1.0 – Initial publication*

Summary

On October 29 and 30, 2024, QNAP released patches for two critical zero-day vulnerabilities, **CVE-2024-50387** and **CVE-2024-50388**, affecting NAS devices. These vulnerabilities allow remote attackers to gain root access and execute arbitrary commands on compromised devices [1,2].

Technical Details

The vulnerability **CVE-2024-50387** in QNAP's SMB service could allow remote attackers to exploit the NAS system and potentially gain a root shell [1,3].

The vulnerability **CVE-2024-50388** could allow remote attackers to execute arbitrary commands on affected devices [2,4].

Affected Products

CVE-2024-50387

- SMB Service before version 4.15.002
- SMB Service before version h4.15.002

CVE-2024-50388

- HBS 3 Hybrid Backup Sync before version 25.1.1.673

Recommendations

CERT-EU recommends applying updates to the affected devices as soon as possible.

References

[1] https://www.qnap.com/fr-fr/security-advisory/qsa-24-42

[2] https://www.qnap.com/fr-fr/security-advisory/qsa-24-41

[3] https://www.bleepingcomputer.com/news/security/qnap-fixes-nas-backup-software-zero-day-exploited-at-pwn2own/

[4] https://www.bleepingcomputer.com/news/security/qnap-patches-second-zero-day-exploited-at-pwn2own-to-get-root/