QNAP, nota marca produttrice di NAS, rende noto che è in corso una una campagna ransomware, denominata *eChoraix;* tale virus è sviluppato per prendere di mira i loro dispositivi NAS vulnerabili o tramite brute-force delle password deboli utilizzate nei dispositivi. Una volta ottenuto l'accesso, gli utenti malintenzionati installano un malware di tipo ransomware che cifra i dati richiedendo il riscatto per ottenere la chiave di decriptazione.

QNAP ha rilasciato un avviso riguardante tre vulnerabilità, identificate rispettivamente con CVE 2018-19943, CVE-2018-19949 e CVE-2018-19953, che consentirebbero di iniettare codice malevolo e/o eseguire codice da remoto. Le vulnerabilità hanno interessato le seguenti versioni:

QTS 4.4.1: build 20190918 e versioni successive;
QTS 4.3.6: build 20190919 e versioni successive;
QTS 4.4.1: Photo Station 6.0.3 e successive;
QTS 4.3.4 - QTS 4.4.0: Photo Station 5.7.10 e successive;
QTS 4.3.0 - QTS 4.3.3: Photo Station 5.4.9 e successive;
QTS 4.2.6: Photo Station 5.2.11 e successive.

QNAP consiglia di aggiornare QTS all'ultima versione disponibile per garantire che il dispositivo possa beneficiare delle correzioni di vulnerabilità. Nel caso in cui si fosse già proceduto all'aggiornamento, come raccomandato dal precedente alert sull'argomento, il rischio di cadere vittima del ransomware di eChoraix sarebbe già stato eliminato. In caso contrario, si consiglia di aggiornare il firmware QNAP all'ultima versione disponibile e di abilitare "Network Access Protection" per proteggere gli account dagli attacchi di brute-force.

Consigliamo di contattare il proprio fornitore hardware o assistenza software.