QNAP emitió un nuevo aviso en el que advierte a los usuarios de sus dispositivos de almacenamiento conectado a la red (NAS) para que actualicen a la última versión de Photo Station después de otra ola de ataques del ransomware DeadBolt al explotar una vulnerabilidad de día cero en el software.

La compañía taiwanesa dijo que detectó los ataques el 3 de septiembre y que *«la campaña parece apuntar a los dispositivos NAS de QNAP que ejecutan Photo Station con exposición a Internet».*

El problema se solucionó en las siguientes versiones:

QTS 5.0.1: Photo Station 6.1.2 y posterior
QTS 5.0.0/4.5.x: Photo Station 6.0.22 y posterior
QTS 4.3.6: Photo Station 5.7.18 y posterior
QTS 4.3.3: Photo Station 5.4.15 y posterior
QTS 4.2.6: Photo Station 5.2.14 y posterior

Los detalles de la vulnerabilidad no están claros hasta ahora, y la compañía aconseja a los usuarios que deshabiliten el reenvío de puertos en los routers, evitar que los dispositivos NAS sean accesibles a Internet, que actualicen el firmware del NAS, apliquen contraseñas seguras para las cuentas de usuario y realicen copias de seguridad periódicas para evitar la pérdida de datos.

El último desarrollo marca la cuarta ronda de ataques DeadBolt dirigidos a dispositivos QNAP desde enero de 2022, seguida de incursiones similares en mayo y junio.

> *«El NAS de QNAP no debe estar conectado directamente a Internet. Recomendamos a los usuarios que utilicen la función MyQNAPcloud Link proporcionada por QNAP, o habiliten el servicio VPN. Esto puede fortalecer el NAS de forma efectiva y disminuir la posibilidad de ser atacado»*, dijo la compañía.