Una nueva variedad de ransomware llamada Qlocker, se dirige a los dispositivos de almacenamiento conectado a la red (NAS) de QNAP, como parte de una campaña en curso y encripta archivos comprimiéndolos en 7zip protegidos con contraseña.

Los primeros informes de las infecciones surgieron el 20 de abril, y los atacantes detrás de las operaciones exigieron un pago de 0.01 Bitcoin para recibir la clave de descifrado.

En respuesta a los ataques en curso, la compañía taiwanesa publicó un aviso en el que se solicita a los usuarios que apliquen actualizaciones al NAS de QNAP con Consola Multimedia, Complemento de Transmisión de Medios y HBS 3 Hybrid Backup Sync, para proteger los dispositivos de cualquier ataque.

> *«QNAP insta encarecidamente que todos los usuarios deben instalar inmediatamente la versión más reciente de Malware Remover y realizar la exploración en el QNAP NAS. Las aplicaciones Consola Multimedia, Complemento de Transmisión de Medios y Sincronización de Copia de Seguridad Híbrida, deben actualizarse a la última versión disponible para proteger aún más el NAS de QNAP de los ataques de ransomware»,* dijo la compañía.

QNAP lanzó parches para las tres aplicaciones durante la última semana. CVE-2020-36195 se refiere a una vulnerabilidad de inyección de SQL en QNAP NAS que ejecuta la Consola Multimedia o el Complemento de transmisión de medios, cuya explotación exitosa podría resultar en la divulgación de información.

Por otro lado, CVE-2021-28799 se relaciona con una vulnerabilidad de autorización incorrecta que afecta al NAS de QNAP que ejecuta HBS 3 Hybrid Backup Sync, que podría ser aprovechado por un atacante para iniciar sesión en un dispositivo.

Parece que Qlocker no es la única variedad que se está utilizando para cifrar dispositivos NAS, ya que los hackers implementan otro ransomware llamado eCh0raix para bloquear datos confidenciales. Desde su lanzamiento en julio de 2019, la banda de eCh0raix es

conocida por perseguir los dispositivos de almacenamiento de QNAP aprovechando vulnerabilidades conocidas o llevando a cabo ataques de fuerza bruta.

> *«Se recomienda a los usuarios que modifiquen el puerto de red predeterminado 8080 para acceder a la interfaz operativa del NAS. Los datos almacenados en el NAS deben respaldarse nuevamente utilizando la regla de respaldo 3-2-1, para garantizar la integridad y seguridad de los datos»,* dijo la empresa.