Los dispositivos de almacenamiento conectado a la red (NAS) de ASUSTOR, se han convertido en el último objetivo del ransomware Deadbolt, menos de un mes después de que ataques similares afectaran a los dispositivos NAS de QNAP.

En respuesta a las infecciones, la compañía lanzó actualizaciones de firmware (ADM 4.0.4.RQ02) para *«solucionar problemas de seguridad relacionados»*. La compañía también insta a los usuarios a tomar las siguientes medidas para mantener la seguridad de los datos:

- Cambiar la contraseña
- Usar una contraseña segura
- Cambiar los puertos HTTP y HTTPS predeterminados. Los puertos predeterminados son 8000 y 8001 respectivamente
- Cambiar los puertos del servidor web (los puertos predeterminados son 80 y 443)
- Apagar los servicios de Terminal/SSH y SFTP y otros servicios que no se usen
- Realizar copias de seguridad periódicas y asegurarse de que las copias estén actualizadas

Los ataques afectan principalmente a los modelos ASUSTOR NAS expuestos a Internet que ejecutan sistemas operativos ADM, incluidos entre otros, AS5104T, AS5304T, AS6404T, AS7004T, AS5202T, AS6302T y AS1104T.

Al igual que las intrusiones dirigidas a los dispositivos NAS de QNAP, los atacantes aseguran estar utilizando una vulnerabilidad de día cero para cifrar los dispositivos NAS de ASUSTOR y exigen que las víctimas paguen 0.003 Bitcoins para recuperar el acceso.

Los operadores de ransomware, en un mensaje separado para ASUSTOR, dijeron que están dispuestos a compartir detalles de la vulnerabilidad si la empresa realiza un pago con bitcoin de 7.5 BTC, además de vender la clave de descifrado universal por un pago total de 50 BTC.

Los detalles exactos de la vulnerabilidad de seguridad utilizada no están claros, pero se sospecha que el vector de ataque se relaciona con una falla en la función EZ Connect que permite el acceso remoto a los dispositivos NAS, ya que la compañía ha instado a desactivar

la función como medida preventiva.

Se recomienda a los usuarios que ya tienen sus dispositivos NAS comprometidos con el ransomware que sigan los siguientes pasos:

- Desconectar el cable de red Ethernet
- Apagar la NAS de forma segura manteniendo presionado el botón de encendido durante tres segundos
- No inicializar la NAS ya que esto borrará los datos
- Rellenar este formulario.