Distintas vulnerabilidades de día cero en grabadoras de video digital (DVR) para sistemas de vigilancia fabricados por LILIN, con sede en Taiwán, están siendo explotadas por operadores de botnets para infectar y cooptar dispositivos vulnerabilidades en una familia de bots de denegación de servicio.

Estos hallazgos provienen del equipo de investigadores de Netlab, de la compañía de seguridad china Quihoo 360, quienes afirman que diferentes grupos de ataque han estado utilizando vulnerabilidades 0-day de LILIN DVR para difundir las botnets Chalubo, FBot y Moobot al menos desde el 30 de agosto de 2019.

Los investigadores de Netlab aseguran los hackers llegaron a LILIN el 19 de enero de 2020, aunque no fue hasta un mes después que el proveedor lanzó una actualización de firmware (2.0b60_20200207) para abordar las vulnerabilidades.

El desarrollo se produce a medida que los dispositivos IoT se utilizan cada vez más como una superficie de ataque para lanzar ataques DDoS y como representantes para participar en distintas formas de cibercrimen.

Vulnerabilidades de día cero

La falla se refiere a una cadena de vulnerabilidades que hacen uso de credenciales de inicio de sesión codificadas (root/icatch99 y report/8Jg0SR8K50), lo que potencialmente le otorga al atacante la capacidad de modificar el archivo de configuración de un DVR e inyectar comandos de puerta trasera cuando el servidor FTP o NTP tienen sincronizadas sus configuraciones.

En un escenario separado, los investigadores descubrieron que el proceso responsable de la sincronización horaria NTP (NTPUpdate), no verifica si existen caracteres especiales en el servidor pasados como entrada, lo que hace posible que los atacantes puedan inyectar y ejecutar comandos del sistema.

La nueva versión parcheada soluciona los defectos al validar el nombre de host para evitar la

ejecución de comandos.

Netlab informó que los operadores detrás de la botnet Chalubo fueron los primeros en explotar la vulnerabilidad NTPUpdate para secuestrar los DVR LILIN en agosto pasado. Posteriormente, se encontró la botnet FBot utilizando las fallas FTP/NTP a inicios de enero. Dos semanas después, Moobot comenzó a propagarse por medio de la vulnerabilidad FTP de día cero de LILIN.

Los investigadores afirmaron que contactaron a LILIN dos veces, primero después de los ataques de FBot, y luego una segunda vez luego de que ocurrieron las infecciones de Moobot.

Aunque Netlab no entró en detalles de los motivos detrás de las infecciones, no sería sorprendente si fueran utilizados por actores de amenazas para realizar ataques distribuidos de denegación de servicio (DDoS) en sitios web y servicios DNS.

> *«Los usuarios de LILIN deben verificar y actualizar los firmwares de sus dispositivos de forma oportuna, y se deben aplicar credenciales de inicio de sesión sólidas para el dispositivo»,* dijo Netlab.