Se encontró una vulnerabilidad de seguridad que afecta a distintas versiones de Through Tek Kalay P2P Software Development Kit (SDK), que podría ser abusada por hackers remotos para tomar el control de un dispositivo afectado y potencialmente conducir a la ejecución remota de código.

Rastreada como CVE-2021-28372, con puntaje CVSS de 9.6 y descubierta por FireEye Mandiant a fines de 2020, la vulnerabilidad se refiere a una falla de control de acceso inadecuado en los productos Through Tek P2P, cuya explotación exitosa podría resultar en la *«capacidad para escuchar audio en vivo, ver datos de video en tiempo real y comprometer las credenciales del dispositivo para futuros ataques basados en la funcionalidad del dispositivo expuesto».*

> *«La explotación exitosa de esta vulnerabilidad podría permitir la ejecución remota de código y el acceso no autorizado a información sensible, como las transmisiones de audio/video de la cámara»,* dijo la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) en un aviso.

Existen al rededor de 83 millones de dispositivos activos en la plataforma Kalay. Las siguientes versiones de Kalay P2P SDK se ven afectadas:

- Versiones 3.1.5 y anteriores
- Versiones del SDK con la etiqueta nossl
- Firmware del dispositivo que no usa AuthKey para la conexión IOTC
- Firmware del dispositivo que utiliza el móvilo AVAPI sin habilitar el mecanismo DTLS
- Firmware del dispositivo usando P2PTunnel o módulo RDT

La plataforma Kalay de la compañía taiwanesa es una tecnología P2P que permite a las cámaras IP, cámaras ligeras, monitores para bebés y otros productos de videovigilancia habilitados para Internet manejar la transmisión segura de archivos de audio y video de gran tamaño con baja latencia. Esto es posible por medio del SDK, una implementación del protocolo Kalay, que está integrado en aplicaciones móviles y de escritorio y dispositivos IoT

en red.

CVE-2021-28372 reside en el proceso de registración entre dispositivos y aplicaciones móviles, específicamente en el modo en que acceden y entran a la red Kalay, permitiendo a los atacantes utilizar un identificador de dispositivo (UID) apócrifo, causando la registración de servidores para sobrescribir el dispositivo existente y trazar conexiones erróneas a otro dispositivo.

> *«Una vez que un atacante ha registrado maliciosamente un UID, cualquier intento de conexión del cliente para acceder al UID de la víctima será dirigido al atacante. El atacante puede seguir el proceso de conexión y obtener los materiales de autenticación necesarios para acceder al dispositivo. Con las credenciales comprometidas, un atacante puede usar la red Kalay para conectarse remotamente al dispositivo original, acceder a dato AV y ejecutar llamadas RPC»,* dijeron los investigadores.

Sin embargo, cabe mencionar que un atacante requeriría un *«conocimiento integral»* del protocolo Kalay, sin mencionar obtener los UID de Kalay por medio de ingeniería social u otras vulnerabilidades en API o servicios que podrían aprovecharse para realizar los ataques.

Para mitigar cualquier posible explotación, se recomienda actualizar el protocolo Kalay a la versión 3.1.10, así como habilitar DTLS y AuthKey para proteger los datos en tránsito y agregar una capa adicional de autenticación durante la conexión del cliente.

Este desarrollo marca la segunda vez que se revela una vulnerabilidad similar en el P2P SDK de Through Tek. En junio de 2021, CISA emitió una advertencia de alerta sobre una vulnerabilidad crítica (CVE-2021-32934) que podría aprovecharse para acceder a las señales de audio y video de la cámara de forma maliciosa.