Se han revelado múltiples vulnerabilidades de seguridad en los sistemas de chips (SoC) de MediaTek, que podrían haber permitido a un actor de amenazas elevar los privilegios y ejecutar código arbitrario en el firmware del procesador de audio, permitiendo efectivamente a los atacantes llevar a cabo una *«campaña de escucha masiva sin el consentimiento de los usuarios».*

El descubrimiento de las fallas es el resultado de la ingeniería inversa de la Unidad de Procesador de Señal Digital de Audio (DSP) de la compañía taiwanesa por parte de la firma israelí de seguridad cibernética Check Point Research, y finalmente descubrió que al unirlas con otras vulnerabilidades presentes en las bibliotecas de un fabricante de smartphones, los problemas descubiertos en el chip podrían conducir a una escalada de privilegios local desde una aplicación de Android.

> *«Un atacante podría utilizar un mensaje entre procesadores mal formado para ejecutar y ocultar código malicioso dentro del firmware DSP. Debido a que el firmware del DSP tiene acceso al flujo de datos de audio, un ataque al DSP podría potencialmente usarse para espiar al usuario»,* dijo el investigador de Check Point Slava Makkaveev.

Rastreadas como CVE-2021-0661, CVE-2021-0662 y CVE-2021-0663, las tres vulnerabilidades se refieren a un desbordamiento de búfer basado en montón en el componente DSP de audio, que podría explotarse para lograr privilegios elevados. Los defectos afectan a los conjuntos de chips MT6779, MT6781, MT6785, MT6853, MT6853T, MT6873, MT6875, MT6877, MT6883, MT6885, MT6889, MT6891, MT6893 y MT8797 que abarcan las versiones 9.0, 10.0 y 11.0 de Android.

> *«En el audio DSP, existe una posible escritura fuera de los límites debido a una grada con comprobación incorrecta. Esto podría llevar a una escalada local de privilegios a privilegios de ejecución del sistema necesarios. No se necesita la interacción del usuario con fines de explotación»,* dijo el fabricante de chips el mes

> pasado.

Un cuarto problema descubierto en la capa de abstracción de hardware de audio de MediaTek, también conocido como HAL (CVE-2021-0673), se solucionó en octubre y se espera que se publique en el Boletín de Seguridad de MediaTek de diciembre de 2021.

En un escenario de ataque hipotético, una aplicación maliciosa instalada a través de medios de ingeniería social podría aprovechar su acceso a la API AudioManager de Android para apuntar a una biblioteca especializada, llamada Android Aurisys HAL, que está aprovisionada para comunicarse con los controladores de audio en el dispositivo y enviar mensajes especialmente diseñados, lo que podría resultar en la ejecución de código de ataque y el robo de información relacionada con el audio.

MediaTek capturó un récord del 43% de todos los envíos de SoC de teléfonos inteligentes para el segundo trimestre de 2021, con sus procesadores utilizados por varios fabricantes de equipos originales como Xiaomi, Oppo, Vivo, Sony y Realme, lo que significa que las vulnerabilidades, si no se abordan, podrían representar una gran superficie de ataque para los hackers.

MediaTek, después de la divulgación, dijo que ha puesto las mitigaciones apropiadas a disposición de todos los fabricantes de equipos originales, y agregó que no encontró evidencia de que las vulnerabilidades estén siendo explotadas actualmente. Además, la compañía recomendó a los usuarios que actualicen sus dispositivos a medida que estén disponibles los parches y que solo instalen aplicaciones de mercados confiables como Google Play Store.