Se revelaron tres vulnerabilidades de seguridad en los decodificadores de audio de los chips Qualcomm y Media Tek, que de no ser resueltos, pueden permitir que un hacker obtenga acceso remoto a los medios y las conversaciones de audio desde los dispositivos móviles afectados.

Según la compañía de ciberseguridad israelí, Check Point, los problemas podrían usarse como una plataforma de lanzamiento para llevar a cabo ataques de ejecución remota de código (RCE) simplemente enviando un archivo de audio especialmente diseñado.

> *«El impacto de una vulnerabilidad RCE puede variar desde la ejecución de malware hasta que un atacante obtenga el control de los datos multimedia de un usuario, incluyendo la transmisión desde la cámara de una máquina comprometida»,* dijeron los investigadores.

> *«Además, una aplicación de Android sin privilegios podría usar estas vulnerabilidades para escalar sus privilegios y obtener acceso a los datos de los medios y las conversaciones de los usuarios»,* agregaron.

Las vulnerabilidades tienen su orgines en un formato de codificación de audio desarrollado originalmente y de código abirto por Apple en 2011. Llamado Apple Lossless Audio Codec (ALAC) o Apple Lossless, el formato de códec de audio se utiliza para la compresión de datos sin pérdida de música digital.

Desde entonces, varios proveedores externos, incluyendo Qualcomm y MediaTek, incorporaron la implementación del códec de audio de referencia proporcionado por Apple como base para sus propios decodificadores de audio.

Y aunque Apple ha parcheado y corregido constantemente las vulnerabilidades de seguridad en su versión patentada de ALAC, la variante de código abierto del códec no ha recibido una

sola actualización desde que se subió a GitHub hace 11 años, el 27 de octubre de 2011.

Las vulnerabilidades descubiertas por Check Point se relacionan con este código ALAC portado, dos de los cuales fueron identificados en procesadores MediaTek y uno en conjuntos de chips Qualcomm:

- CVE-2021-0674, con puntaje CVSS de 5.5 (MediaTek): Un caso de validación de entrada incorrecta en el decodificador ALAC que conduce a la divulgación de información sin interacción del usuario.
- CVE-2021-0675, con puntaje CVSS de 7.8 (MediaTek): Una vulnerabilidad de escalada de privilegios local en el decodificador ALAC derivada de una escritura fuera de los límites.
- CVE-2021-30351, con puntaje CVSS de 9.8 (Qualcomm): Una acceso a la memoria fuera de límite debido a una validación incorrecta de la cantidad de cuadros que se pasan durante la reproducción de música.

En un exploit de prueba de concepto ideado por Check Point, las vulnerabilidades permitieron *«robar el flujo de la cámara del teléfono»,* dijo el investigador de seguridad Slava Makkaveev, a quien se le atribuye el descubrimiento de las vulnerabilidades, en conjunto con Netanel Ben Simon.

Después de la divulgación responsable, los respectivos fabricantes de chips cerraron las tres vulnerabilidades en diciembre de 2021.

> *«Las vulnerabilidades eran fácilmente explotables. Un actor de amenazas podría haber enviado una canción (archivo multimedia) y cuando una víctima potencial la reproduce, podría haber inyectado código en el servicio de medios privilegiado. El actor de amenazas podría haber visto lo que ve el usuario del teléfono móvil en su teléfono»,* dijo Makkaveev.